AI agents inside the finance department

What they can read, what they can change, and who approves

IN BRIEF

01 Finance is the department where an agent's mistake does not stay a mistake. It becomes a payment, a posted journal or a filed return. That is why the question to ask first is not where an agent runs. It is who approves.

02 The suppliers answer that question differently, and in public. One payables vendor says: "Authorized people retain control of approvals, exception resolution, ERP posting, and payment release." Another says its agents review every expense report, "approving, rejecting, or requesting changes". A published workflow template has a path named "Auto-Approve (<$5K + Low Risk)". Hosting separates them less: two of the vendor pages we read offer an on-premises option in so many words.

03 The fraud record explains why approval matters. The FBI's internet crime centre recorded losses of more than three billion dollars to business email compromise in the United States in 2025. One engineering firm lost about 25 million dollars after a video call with a false finance chief. In both, a person was persuaded to pay. An agent that acts on an email or a call can be persuaded too.

04 This paper is about the finance department's own work: the reading, matching, checking and drafting done in payables, the vendor file, receivables, the close, reporting, treasury, expenses, tax and control. It sets out what an agent can read, how it reaches finance systems, what it may change without a person, and what the rules on internal control, payments and decisions about people already say. It ends with seven questions to put to any supplier, and with a place to start.

05 The position throughout is simple. An agent prepares. A named person decides. No agent pays, releases a payment run, posts a journal, changes a vendor's bank details, approves an expense or files a return. Each agent has one job, one owner and a record, because it sits inside the controls the finance director answers for. The agent runs on infrastructure the company controls.

IN THIS PAPER

01 Where finance departments are today 2
02 The work nobody has packaged 3
03 Three doors, one gate 4
04 What an agent may do 5
05 What the rules already ask 6
06 A worked example: one mid-sized manufacturer's finance team 8
07 Seven questions before an agent touches a payment 9
08 Where to start 9

PART 01

Where finance departments are today

74%

of organisations affected by business email compromise in 2025, in a treasury survey

$25M

lost by one engineering group after a video call with a false finance chief

The suppliers have arrived, and most began with the invoice. Vendor pages now describe agents for invoice capture and matching, expenses, collections, reconciliation and the close. Workday announced finance agents in September 2025, one of them for audit evidence collection and reporting [8]. Suppliers publish their own figures for time saved. We found no named, dated, independently measured result for a finance agent, and this paper quotes none as proof.

They disagree on who approves. This is the clearest difference in the published material.

- Stampli answers the question on its own page. “Does Billy make final decisions or approve transactions? No.” Then: “Authorized people retain control of approvals, exception resolution, ERP posting, and payment release” [1].
- AppZen says its agents “review 100% of expense report and card transactions, approving, rejecting, or requesting changes, and looping in humans when real judgment is needed” [2].
- One published workflow template routes invoices by a risk score from a hosted model. Its third path reads: “Auto-Approve (<$5K + Low Risk)”. It lists “Configurable auto-approve limits” as a feature [3].
- Another template says “Small, clean, PO-matched invoices approve themselves”, and adds a rule worth copying: “Whoever raised the PO never approves its invoice” [3].
- Microsoft’s reconciliation agent for its finance system recommends an action for each exception. “You can either accept that recommendation or select from other available actions” [5].

None of these is wrong for every company. They are different answers, and a buyer should know which one it is buying.

Hosting separates them less than buyers expect. Automation Anywhere’s datasheet for its payables product lists “Private cloud (AWS, Google Cloud, Microsoft Azure), hybrid, or fully on-prem” [4]. Nanonets lists “VPC, single-tenant cloud, or on-prem” [4]. Most of the other pages we read do not say where the agent runs. One says its AI features need a setting switched on: “the existing Move data across regions setting must be enabled for the environment” [5]. So where it runs is still a question to ask. It is not the question that tells suppliers apart.

The loss record is about people being persuaded. The FBI’s Internet Crime Complaint Center put losses to business email compromise at $3,046,598,558 in 2025, against $2,770,151,146 in 2024 [6]. It describes the scam as one “targeting businesses or individuals working with suppliers and/or businesses regularly performing wire transfer payments”. It notes that AI is a small part so far: “In 2025, businesses reported losses over $30 million to BEC scams involving AI” [6].

A survey of treasury staff says the same. The Association for Financial Professionals reported in April 2026: “About three in four organizations (74%) were affected by business email compromise (BEC) in 2025” [7].

One case shows what a convincing call can do. In May 2024 CFO Dive reported that the engineering group Arup lost “approximately $25 million”. A staff member received a message that claimed to come from the chief financial officer, joined a video conference with a false one, and “made a number of transactions to five different Hong Kong bank accounts” [9]. No software was at fault. A request was believed, and nobody independent checked it.

What the published accounts leave out. Few of the pages we read say what happens when a vendor asks to be paid into a different bank account. One vendor says its agent holds such a change “for authorized review” [1]. One template says “Changed bank details alert finance” [3]. Most say nothing.

We found no public account of an agent paying a wrong or a duplicate invoice, and we do not claim one.

PART 02

The work nobody has packaged

All three
templates we opened approve some invoices with no person involved

Hosted
services are what all three are built from: model, mailbox, spreadsheet, accounting system

We listed the jobs a finance department does and looked for each in the template libraries and prebuilt agents of the agent and workflow platforms. They are thick around the supplier invoice. They thin out wherever the work is a check before a person signs.

WHERE TEMPLATES OR PREBUILT AGENTS EXIST	WHERE NONE WAS FOUND
An invoice read, checked for a duplicate and approved or routed	**A supplier's statement compared with the payables ledger**
An invoice from a mailbox turned into a bill in the accounting system	**A payment run checked, before release, for what changed since the last one**
An approval task created for a person, with the invoice attached	**Balances that two group companies record differently, listed with the likely cause**
A ledger and sub-ledger exception given a recommended action	**A loan covenant worked out against the agreement's own definitions**
Expense reports reviewed, approved or rejected	**A draft board pack checked for figures that disagree between pages**
Overdue accounts ranked and a follow-up email written	**The working papers for a VAT or sales tax return**
Audit evidence collected and reported	**Sections of a transfer pricing file drafted from the agreements**

Two findings matter more than the list. First, the templates we opened decide. All three approve some invoices with no person involved: one "Auto-approves low-value, low-risk invoices", one has the path named above, and in the third small matched invoices "approve themselves" [3]. The limit is a setting. Whoever sets it has written a payment control, whether or not the controller knows.

Second, all three are built from hosted services: a hosted model, a hosted mailbox, a hosted spreadsheet, a hosted accounting system. That settles where supplier invoices and bank details go before anyone has asked [3].

The gaps sit where the reading is slow and the signature already belongs to a named member of the finance team. That makes them the safer place to begin.

PART 03

Three doors, one gate

An agent is only as useful as what it can reach. In a finance department that means three kinds of thing.

Documents.

The accounting manual, the purchasing and expense policies, the delegation of authority, loan agreements, supplier contracts. These are indexed once as knowledge sources, with each reader's permissions kept, so an agent answers with the paragraph it relied on and says when the documents are silent.

Systems of record.

The ledger, payables, receivables, the vendor file, bank balances. Most are reached through an interface the company already runs. The company gives the platform the description of that interface, chooses which operations become tools, and decides which of them need approval.

Closed figures and transactions for analysis.

Actuals, budget, payment history, payroll totals and tax transactions, held in the data warehouse or a reporting database, and read only.

All three pass one gate: every tool call is checked against the company's policy, which can allow it, record it, hold it for a person, or block it.

Where the company's interface checks the caller, the agent acts as the person using it and cannot claim another.

SIX WAYS INTO A FINANCE DEPARTMENT'S SYSTEMS

	ROUTE	WHAT IT REACHES	WHAT TO KNOW
01	**A file the user uploads**	An invoice, a bank statement, a supplier statement, an expense claim, a contract	Nothing is connected. The safest start
02	**A knowledge source**	The accounting manual, policies, the delegation of authority, loan agreements	Permissions are kept per reader
03	**An imported description of an interface**	The ledger, payables, receivables, the vendor file, bank balances	You choose the operations. Changes wait for approval
04	**A reporting database**	Closed figures, budget, payment history, payroll totals, tax transactions	Read only
05	**A server from the tool catalogue, run in your cluster**	Databases, web search, document conversion	It runs inside; check what each tool does
06	**Public sources**	Tax authorities' rules, regulators' guidance, filed company accounts	Reads only, from the publisher

PART 03 · CONTINUED

196

public interface descriptions read, from 23 publishers; 159 import

3,510

of the 6,199 operations in the 159 that import are sent as changes

What is published. We read 196 public interface descriptions from 23 publishers and ran each through the platform's importer. 159 import. 30 are refused for an old format, and 7 are over the size limit. The 159 carry 6,199 operations, of which 3,510 are sent as changes, and the method alone cannot tell which only read. One bank-data interface sends 346 of its 351 operations as changes, although most of them only read [10].

What that exercise taught us. The open interfaces in finance are built to do things: take a payment, issue a refund, create a payee, raise a bill. More than half of the operations are sent as changes, and some of those only read.

What is not published. The 23 publishers are payment providers, card and spend platforms, billing systems, bank-access standards, one tax engine, one tax authority and small-business accounting. No large ERP publishes a description a file address reaches. Nor does any consolidation, treasury or procurement system we looked for. For those, the description comes from the company's own system, or the agent reads from the data warehouse.

Bank credentials and the release. The safe design keeps the agent on the preparing side. It holds no bank token and no second factor, and it releases nothing.

So choose the operations at import, read what each one does, start with the ones that only read, and add nothing that pays, posts or changes a vendor until the approval step has been seen working.

PART 04

What an agent may do

One rule runs through every agent in this paper: it prepares, and a named person decides.

01	**It reads** what the person using it could read, and no more.
02	**It drafts** the reconciliation, the variance commentary, the reminder, the working papers, with each figure tied to its source.
03	**It lists** what does not match, what is missing, what changed since last time, and what falls due.
04	**It stops** before anything that moves money, changes a record or leaves the company. A tool that changes something waits for approval.
05	**It does one job.** An agent is given the tools for one duty. The agent that reads a bank detail request holds no tool that changes the vendor file or releases a payment.
06	**It decides nothing about a person.** It does not approve or reject a colleague's claim, does not score an employee, and sets no individual's credit.

PART 04 · CONTINUED

That gives 35 agents in nine areas: accounts payable; the vendor file and purchasing; receivables and collections; close and reconciliation; reporting and planning; treasury and cash; expenses and payroll checks; tax and e-invoicing; control, audit and fraud. The full list is a separate document. Four lines are drawn tighter than the rest.

Payments and bank details.

An agent may match an invoice to its order and receipt, list likely duplicates, and set out what changed in a payment run since the last one: new payees, changed bank details, amounts above the usual. It may take a request to change where a vendor is paid, compare it with the record and the request's history, and prepare the call-back sheet. It pays nothing and releases nothing. A person calls the vendor on a number the company already holds, a second person approves the change, and the payments approver releases every run.

The ledger.

An agent may propose bank matches, prepare a balance sheet reconciliation, and list manual journals that need a second look: no support, a round amount, an unusual pair of accounts. It posts and reverses nothing. The preparer signs, the reviewer approves, and the controller reviews each journal.

What leaves the company.

An agent may draft a reminder, a monthly pack, a covenant calculation, the working papers for a return, or the replies to an auditor's request list. It sends, files and submits nothing. The credit controller sends the reminder. The tax manager files the return. The controller releases what goes to the auditor.

People.

An agent may check an expense claim against the policy and cite the rule, or list payroll differences that have no stated cause. It approves no claim and assesses no employee. The credit review agent is for business customers; it prepares the file and a credit manager sets every limit.

PART 05

What the rules already ask

This part needs a lawyer's read, and an auditor's, before it is relied on. It reports what the texts say; it is not advice. Nothing in it says that a platform makes a company compliant. Controls belong to the company.

Internal control over financial reporting

Officers sign for the controls. Under section 302 of the Sarbanes-Oxley Act, the officers who sign a United States issuer's reports certify that they "are responsible for establishing and maintaining internal controls" and "have evaluated the effectiveness of the issuer's internal controls as of a date within 90 days prior to the report" [11].

Weaknesses are reported. The same section has them disclose to the auditors and the audit committee "all significant deficiencies in the design or operation of internal controls" [11].

Management assesses, and the auditor attests. Under section 404 the annual report must "contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting" [11].

The United Kingdom now asks boards for a declaration. The Financial Reporting Council says of its 2024 Code: "Provision 29 now asks boards to make a declaration in relation to the effectiveness of their material internal controls" [12]. The Code works on a "comply or explain" basis. We read the Council's page, not the Provision's own text.

What this means for an agent. None of these texts mentions AI. They do not need to. An agent that matches, reconciles or prepares evidence is a part of the control environment, like a report or a spreadsheet the team relies on. Someone must own it. Its job must be stated. Changes to it must be approved, and what it did must be on record for the person who tests the control. An agent with no owner and no record is a gap the finance director signs over.

Auditors keep a person accountable in their own work. In March 2026 the Financial Reporting Council published guidance for audit firms on generative and agentic AI. Its announcement says: "As set out in auditing standards, the human auditor is always accountable" [13]. That is a rule for audit firms, not for the companies they audit. It shows what the auditor across the table will expect.

PART 05 · CONTINUED

Payments and fraud

The bank now checks the name. Regulation (EU) 2024/886 says: "A payer's PSP shall offer the payer a service ensuring verification of the payee to whom the payer intends to send a credit transfer." The check runs "before the payer is offered the possibility of authorising that credit transfer" [14]. Where the name and the account do not match, the bank tells the payer. The decision to go on is then the payer's, so it should be a person's.

American payment rules ask originators to screen for fraud. Nacha's rules for the ACH network now ask each non-consumer originator to "establish and implement risk-based processes and procedures" that are "reasonably intended to identify Entries that are suspected of being unauthorized or authorized under False Pretenses" [15]. Nacha defines False Pretenses to include a person misrepresenting "the ownership of an account to be credited". That is the bank-detail change described in plain words.

The loss usually stays with the company. Whether a company that pays a fraudster can recover anything from its bank depends on the market and the contract. That is for counsel. The safe assumption is that the control has to be the company's own.

Decisions about a person

A person decides about a person. Under the GDPR, a person "shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her", with stated exceptions [16]. Whether a rejected expense claim or a sole trader's credit limit falls under these words is for counsel.

Finance is mostly not on the European Union's high-risk list. Credit scoring of individuals is. The AI Act lists as high-risk "AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems used for the purpose of detecting financial fraud" [17]. We found no entry in that list for payables, the close, planning, treasury or tax.

The dates have moved. Regulation (EU) 2026/1744 says the date of application of the high-risk duties "is set to 2 December 2027 for AI systems classified as high-risk pursuant to Article 6(2) and Annex III, and to 2 August 2028 for AI systems classified as high-risk pursuant to Article 6(1) and Annex I" [18]. Credit scoring sits in Annex III, so its date is 2 December 2027.

MARKET	WHAT WE READ	WHAT IT ASKS
United States	Sarbanes-Oxley Act, section 404(b)	The audit firm "shall attest to, and report on, the assessment made by the management of the issuer" [11]
United Kingdom	Financial Reporting Council, Code page	"Provision 29 applies to financial years beginning on or after 1 January 2026" [12]
European Union	Regulation 2024/886, Article 5c(9)	"PSPs located in a Member State whose currency is the euro shall comply with this Article by 9 October 2025" [14]
United States	Nacha, fraud rules, phase two	Each party must "review (at least annually) these processes and procedures", from 22 June 2026 [15]
European Union	Directive 2025/516	Electronic invoices in a "structured electronic format"; the measures "shall apply" from 1 July 2030 [19]

We did not open the auditing standards themselves, the control frameworks, the rules in Japan, the Gulf, India, Singapore or Australia, any country's own e-invoicing dates, or any record retention period. Several of the e-invoicing dates moved in the past year. A company should check each with its own tax adviser.

PART 05 · CONTINUED

What the rules have in common

01	**Named people answer for the controls,** and an auditor tests them.
02	**A weakness is something to report,** so an agent's failures must be visible.
03	**A payment is checked before it is authorised,** and a mismatch goes to a person.
04	**A person decides** anything that judges a person.

PART 06

A worked example: one mid-sized manufacturer's finance team

Take a made-up manufacturer: six legal entities, about 1,400 staff, and a finance team of 38. Nothing here is a customer's story, and every figure is illustrative; it is section 4 put to work.

01

In accounts payable, a supplier sends its month-end statement. The agent compares 212 lines with the payables ledger and lists nine that appear on one side only. A payables clerk follows up each one.

02

At the vendor file, an email asks for a supplier's payments to go to a new bank account. The agent compares the request with the record, lists three things that do not fit, and prepares the call-back sheet. A clerk calls the number already on file. A second person approves the change, or does not.

03

Before the payment run, the agent sets the proposed run of 640 payments against the last one and lists four new payees, two changed bank details and one invoice paid early. The payments approver releases the run.

04

At the close, the agent reads 1,150 manual journals against the accounting manual and lists 23 for a second look. The controller reviews each one.

05

For the treasurer, the agent works out three loan covenants from the quarter's figures and the agreement's definitions, with the headroom and the clause. The treasurer confirms the calculation and reports to the lender.

06

For the audit, the agent takes the auditor's list of 180 requests, finds the document or the report for 163, and marks 17 it could not find. The controller reviews and releases everything that goes.

Every one of these reads documents or records the company already has, changes no record by itself, moves no money, sends nothing outside the company, and leaves a record of who asked and what was shown.

PART 07

Seven questions before an agent touches a payment

01 **Where does it run?**
On our infrastructure, in our private cloud, or in the supplier's service? Where is the model? Does any step send ledger, vendor, bank or payroll data elsewhere, and which?

02 **What can it read?**
Does it act as the person using it, with their permissions, or as one all-seeing account? Can it reach bank credentials or payroll detail?

03 **What can it change?**
Which tools post a journal, change a vendor, approve a claim or release a payment, and does each wait for a person?

04 **Who approves, and is there a limit below which nobody does?**
Show us every threshold, who set it, and who can change it.

05 **Can one agent do both halves of a duty?**
Show us that the agent that reads a bank detail request cannot change the vendor file or release a payment.

06 **What is recorded?**
Who asked, which tool ran, what was decided, for how long is that kept, and can the control owner and the auditor read it?

07 **Can we stop it?**
One agent, one tool, or all of them, at once, by us.

PART 08

Where to start

Pick work where reading is slow, the decision stays with a person, and no money moves on the agent's word.

Accounting policy questions and answers
Colleagues ask what the manual says and get the answer with the paragraph cited. No ledger is touched.

Supplier statement reconciliation
The agent lists each difference between a statement and the ledger. A payables clerk follows up.

Bank detail change check
The agent lists what does not fit and prepares the call-back. Two people make the change.

One entity, one process, invented data first. Then beside the manual process, measured against it.

About Katonic AI

Katonic AI builds the platform that organisations use to build, run and govern AI agents on their own infrastructure: in their own data centre, in a private or sovereign cloud, or with no connection to the internet at all. The platform is in production with governments, banks, telecom operators and utilities. Katonic is certified to ISO 27001.

KATONIC.AI/SOLUTIONS/FINANCE

SOURCES

Read on 22 November 2026. Figures are the publishers' own and were not audited by us.

01 Stampli, "AI" product page (the agent named Billy), undated, read 22 November 2026. https://www.stampli.com/ai/

02 AppZen, home page, undated, read 22 November 2026. https://www.appzen.com/

03 n8n workflow templates 9436 ("Auto-extract & approve invoices with OpenAI, Jotform - fraud detection", last updated about nine months before reading), 20234 ("Approve vendor invoices from Gmail using Claude, Google Sheets, Slack and QuickBooks", last updated about a month before reading) and 19739 ("Process, validate and approve invoices with OpenAI GPT-4o and Google Sheets"). https://n8n.io/workflows/9436-auto-extract-and-approve-invoices-with-openai-jotform-fraud-detection/ ; https://n8n.io/workflows/20234 ; https://n8n.io/workflows/19739-process-validate-and-approve-invoices-with-openai-gpt-4o-and-google-sheets/

04 Automation Anywhere, accounts payable solution datasheet, dated December 2025 in its footer. https://www.automationanywhere.com/sites/default/files/internal-assets/datasheet_ap_solution_r3_en.pdf ; and Nanonets, invoice processing page, undated. https://nanonets.com/invoice-processing

05 Microsoft Learn, "Account Reconciliation Agent (production ready preview)", Dynamics 365 Finance, last updated 10 November 2026. https://learn.microsoft.com/en-us/dynamics365/finance/general-ledger/acct-rec-agent

06 Federal Bureau of Investigation, Internet Crime Complaint Center, "2025 Internet Crime Report" (published 2026; the day was not found in the text). https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

07 Association for Financial Professionals, press release on the 2026 AFP Payments Fraud and Control Survey, 14 April 2026 (465 treasury practitioners, surveyed January 2026). https://www.financialprofessionals.org/about/learn-more/press-releases/Details/over-75-percent-of-us-firms-experienced-payments-fraud-in-2025-while-ai-adoption-for-fraud-mitigation-lags

08 Workday, "Workday Illuminate Expands with New AI Agents for HR, Finance, and Industry", press release, 16 September 2025. https://newsroom.workday.com/2025-09-16-Workday-Illuminate-TM-Expands-with-New-AI-Agents-for-HR%2C-Finance%2C-and-Industry

09 CFO Dive, "Scammers siphon $25M from engineering firm Arup via AI deepfake 'CFO'", 17 May 2024. https://www.cfodive.com/news/scammers-siphon-25m-from-engineering-firm-arup-via-ai-deepfake-cfo/716501/

SOURCES continued

10 Template libraries and prebuilt agents of agent and workflow platforms, searched 22 November 2026 (includes Zapier, “Create invoice approval task with invoice and link”, https://zapier.com/automations/finance/accounts-payable/invoice-processing-management/create-invoice-approval-task-with-invoice-and-link , and Microsoft’s adoption scenario library, “Collections agent”, https://adoption.microsoft.com/scenario-library/finance/collections-agent/); and 196 interface descriptions from 23 publishers fetched the same day and run through the platform’s importer (Katonic research).

11 Sarbanes-Oxley Act of 2002, section 302 (15 U.S.C. § 7241(a)(4) and (5)) and section 404 (15 U.S.C. § 7262(a) and (b)), enacted 30 July 2002. https://www.law.cornell.edu/uscode/text/15/7241 ; https://www.law.cornell.edu/uscode/text/15/7262

12 Financial Reporting Council, “UK Corporate Governance Code” page and its questions and answers on the 2024 Code, read 22 November 2026. https://www.frc.org.uk/library/standards-codes-policy/corporate-governance/uk-corporate-governance-code/

13 Financial Reporting Council, “Innovative new guidance supports audit firm adoption of emerging AI technologies”, news release, 30 March 2026. https://www.frc.org.uk/news-and-events/news/2026/03/innovative-new-guidance-supports-audit-firm-adoption-of-emerging-ai-technologies/

14 Regulation (EU) 2024/886 of 13 March 2024, Article 5c(1) and (9) as inserted in Regulation (EU) No 260/2012. http://publications.europa.eu/resource/celex/32024R0886

15 Nacha, rule page on the phase two fraud rules for the ACH network (page title not copied), effective 19 June 2026 (practical date 22 June 2026). https://www.nacha.org/rules/risk-management-topics-fraud-monitoring-phase-2

16 Regulation (EU) 2016/679 (GDPR), Article 22(1). http://publications.europa.eu/resource/celex/32016R0679

17 Regulation (EU) 2024/1689 (AI Act), Annex III point 5(b). http://publications.europa.eu/resource/celex/32024R1689

18 Regulation (EU) 2026/1744 of 8 July 2026 (Official Journal 24 July 2026), the recital on the dates of application; the operative text gives the same two dates. http://publications.europa.eu/resource/celex/32026R1744

19 Council Directive (EU) 2025/516 of 11 March 2025, the definition of “electronic invoice” and the article on transposition. http://publications.europa.eu/resource/celex/32025L0516