How AI can contribute to bank failure

Adrian Dunkley | 2026-11-18 | Evidence review and stress scenarios

Print edition of the public web text, prepared 20 November 2026. Open the source publication.

By **Adrian Dunkley** · 18 November 2026

A bank can meet its capital requirements and still run out of cash. An unchecked AI draft can delay action on a cash shortfall. A fake message from the chief executive can make customers withdraw money faster.

This review found no public supervisory finding that identifies AI as a primary cause of the failure of a licensed deposit-taking bank. It uses documented incidents to test how AI can add to losses or weaken a bank already under stress.[17] [22] [3]

Open the 100-risk register

What the evidence shows

The review covers research and public records available through 18 November 2026. It draws on selected supervisory reports, case records and studies of lending and office work. The US failed-bank list covers US banks only.[22]

AI adoption is rising where banks depend on suppliers

In the Bank of England and Financial Conduct Authority survey, third parties supplied 39% of reported AI systems in 2026. The share was 33% in 2024. For systems that firms classed as highly important, the share rose from 35% to 53%. These are UK survey results. Respondents and reporting methods changed between rounds. The denominator is reported AI use cases in 2024 and reported AI systems in 2026. The figures measure supplier exposure.[1] [2]

Third-party share of reported AI

UK financial services survey. Percentage of reported systems or use cases in each group.[1] [2]

All reported AI, 2024 · 33%

All reported AI, 2026 · 39%

Higher-importance AI, 2024 · 35%

Higher-importance AI, 2026 · 53%

The Financial Stability Board identifies four routes to wider disruption. Banks can depend on the same suppliers or react to the same market signals. Cyber incidents and model errors can also spread across firms. Its 2025 follow-up calls for better monitoring. The International Monetary Fund identifies deeper liquidity as a possible benefit of AI in normal markets. This means buyers and sellers can trade more easily. In a stressed market, similar signals and faster orders can make trading harder.[3] [4] [5]

AI can improve work and introduce new errors

A study of consultants found that AI improved performance on tasks within the tool’s capabilities. For a task outside those capabilities, users were less likely to give the correct answer. A separate US survey asked desk workers about polished AI output that left other staff to do the work again. The authors call this output workslop. The survey measures workers’ reports across sectors. It gives no bank-level error rate.[13] [14]

In banking, a draft can look complete while it uses the wrong reporting period or omits a large balance. A reviewer must trace material figures to the ledger and check the reporting date. A legal, credit or treasury

specialist must verify conclusions that depend on rules or expert judgement.

A peer-reviewed US mortgage study found price differences between borrowers with similar credit risk. It found that the comparison between fintech and other lenders varied by loan type. This evidence gives banks a reason to test lending decisions by borrower group. US mortgage results cannot measure how a model will perform for Jamaican microbusinesses or remittance earners.[15]

The Bank of Jamaica's November 2026 statement identifies fraud and cyber risk from AI. Its published stress results give no estimate of AI-related bank failure.[24]

Incidents that show how losses spread

Case	Evidence	What happened
Hong Kong payment fraud · 2024	Documented AI use	Hong Kong reported a fake video meeting that led to transfers to five local bank accounts. The victim lost about HK$200 million. This was a corporate fraud case.[18]
Banco Popular Dominicano · 2025	Bank impersonation	The bank reported a false video of its chief executive promoting a fraudulent investment. Its notice gave no customer loss total.[23]
Jamaica payments infrastructure · 2026	Cyber incident	The Bank of Jamaica reported an incident at Jamaica Electronic Transfer Services Limited. MultiLink and the automated clearing house stayed in service. The statement gives no AI attribution.[25]
Knight Capital · 2012	Software failure comparison	A software error produced orders the broker-dealer did not intend to send. The US Securities and Exchange Commission recorded a loss above US$460 million.[19]
CrowdStrike · 2024	Shared supplier comparison	A supplier sent a security software update that caused outages on affected Windows systems. A common dependency gave the update a wide reach.[21]
Silicon Valley Bank · 2023	Bank failure comparison	Customers withdrew more than US$40 billion on 9 March. The Federal Reserve identified management and supervisory failures and weaknesses in liquidity and interest-rate risk management.[20]

The first two cases show how fraudsters used AI. The remaining cases show how a similar failure can spread.

Eight stress scenarios for 2027 to 2029

Bank and method

The reference bank is a mid-sized Caribbean deposit taker with US$2 billion in assets and US$1.6 billion in deposits. It starts with US$260 million in liquid assets that it can use on the same day. It has US$60 million of eligible capital above its applicable minimum. These are assumed balances for an exercise.

The capital buffer is the amount of eligible capital above the minimum. The bank uses third-party AI in some operations and can run a limited set of models locally. It still uses staff and fixed rules for many decisions. Each scenario assumes the exposure named in its trigger. The eight triggers describe possible events in one bank-year under different deployment or market conditions.

Each annual range multiplies two inputs. The first is the assumed chance that the named trigger occurs. The second is the assumed chance of a severe outcome if that trigger occurs. The low ends and high ends give a sensitivity range. Each three-year projection repeats the low or high annual rate and assumes equivalent exposure and independence across years. A prolonged outage, repeated fraud or an unresolved weakness

breaks that assumption.

The sources inform the choice of scenarios and their controls. They do not supply the input probabilities. The author assigns the bands as stress inputs. The study does not fit them to bank incident data. The outcomes differ by row and can overlap. The bank cannot add the rows to get a chance of failure.

Scenario	Route and trigger	Trigger in 1 year	Severe outcome if triggered	Severe outcome in 1 year	Severe outcome in 3 years	Severe outcome threshold
AI agent changes payments	Direct. An AI agent with permission to write to a payments system makes an unauthorised change.[3] [10] [19]	2–6%	5–20%	0.10–1.20%	0.30–3.56%	Payment disruption exceeds four hours or direct loss reaches US$5m.
Deepfake payment fraud	Indirect. Staff receive a credible impersonation linked to a high-value payment.[18] [17]	8–20%	5–15%	0.40–3.00%	1.20–8.73%	Unrecovered fraud loss reaches US$5m.
AI-assisted intrusion	Indirect. A material breach affects the bank or a supplier. An investigation attributes part of the breach to AI.[6] [17] [10]	3–10%	10–25%	0.30–2.50%	0.90–7.31%	A critical service is unavailable for one business day.
Shared AI supplier outage	Indirect. A supplier incident affects two critical bank services at the same time.[21] [2] [4]	4–12%	10–30%	0.40–3.60%	1.20–10.42%	A critical service is unavailable for one business day.
False report and deposit run	Combined. A material liquidity reporting error coincides with a public confidence shock.[20] [14] [9]	1–4%	5–20%	0.05–0.80%	0.15–2.38%	Same-day cash falls short of obligations before emergency funding.
AI investment slump	Indirect. An AI-sector downturn hits a bank with concentrated credit or market exposure.[8] [7]	5–15%	5–20%	0.25–3.00%	0.75–8.73%	Losses exceed the US$60m capital buffer.
Forced move to a local model	Indirect. A local-use mandate affects a critical workflow before the bank finishes testing the fallback.[12] [11] [10]	2–8%	10–30%	0.20–2.40%	0.60–7.03%	A critical service is unavailable for one business day.
Scenario	Route and trigger	Trigger in 1 year	Severe outcome if triggered	Severe outcome in 1 year	Severe outcome in 3 years	Severe outcome threshold
Biased credit at scale	Direct. A credit model fails the bank’s error-rate test for a	8–20%	5–15%	0.40–3.00%	1.20–8.73%	A review finds at least 1,000 decisions that require a new

Scenario	Route and trigger	Trigger in 1 year	Severe outcome if triggered	Severe outcome in 1 year	Severe outcome in 3 years	Severe outcome threshold
	borrower group after launch.[15] [9]					assessment.

One-year chance of a severe outcome

Bars show the low and high estimates. Each row uses its own severity threshold.

Shared AI supplier outage · 0.40–3.60%

Deepfake payment fraud · 0.40–3.00%

AI investment slump · 0.25–3.00%

Biased credit at scale · 0.40–3.00%

AI-assisted intrusion · 0.30–2.50%

Forced move to a local model · 0.20–2.40%

AI agent changes payments · 0.10–1.20%

False report and deposit run · 0.05–0.80%

A liquidity shortfall means the bank cannot meet all payments due from its available cash. A capital breach means eligible capital falls below the applicable minimum. Either can trigger action by the bank or supervisor. The supervisor decides whether to intervene or close a bank under local law. The model estimates neither closure nor resolution.

Worked case. A false report and a rush to withdraw funds

An AI-written treasury report omits a large depositor group. Treasury staff use the draft to set the day’s cash reserve. Later, a false message about the bank’s health circulates while customers have trouble logging in. The bank tells its crisis team to treat the report error and the public claim as one event.

In this stress test, 18% of deposits leave in one day. That is US$288 million. The bank can use US$260 million on the same day. The gap is US$28 million before emergency funding. At a 12% withdrawal rate, US$68 million remains. A loss of US$50 million in same-day access to collateral lowers the rate at which cash runs out to about 13.1% of deposits. Emergency funding can change these results if the bank can draw it in time.

Suppose an accurate morning report lets Treasury make US$30 million more available that day. Keep withdrawals at US$288 million. The gap becomes a US$2 million surplus. This comparison assumes the extra cash is available in time.

• Treasury draft omits deposits

• Staff set a lower cash reserve

• False claim speeds withdrawals

• Cash falls below payments due

Same-day cash in the deposit run

US$ million. Values come from the worked exercise.

Cash in the base stress · 260

Withdrawals at 18% · 288

Cash if Treasury raises another US$30m · 290

Worked case. AI infrastructure loans lose value

Assume a bank lends US$120 million to data centres and related projects. Borrowers draw a further US$40 million from commitments before the shock. At a 30% loss on that balance, the bank loses US$48 million. A separate US$15 million loss on traded assets takes the combined loss to US$63 million.

That loss exceeds the assumed US$60 million buffer by US$3 million, before tax effects or changes in risk-weighted assets. With zero loss on traded assets, a 37.5% loan loss uses up the buffer. This is a simplified sensitivity check. Banks can apply their current capital rules and count each exposure once.[8] [7]

Where AI changes bank strategy

Local control takes more than a local server

AI sovereignty means retaining control over where data goes and who can run or change a service. A policy can require local storage or local processing. It can also limit which suppliers a bank can use. Each choice creates a different operating requirement. In this study, a mandate to use a local model is a hypothetical policy shock.

Local hosting can give a bank more control over sensitive records and access logs. It can also put two recovery sites on the same electricity or telecom network. A locally hosted model can still rely on a foreign provider for updates or software that checks licences. A local model can have little training data for specific loan products. Banks can test the service with local staff, local data and their own products before switching.

The World Bank identifies gaps in computing capacity, connectivity, local data and skills. A bank can share training and testing with regional partners while retaining its own decision rules. For a critical service, ask two named teams to prove they can run and restore it. Test the fallback during hurricane conditions or when a key staff member is unavailable. The Bank of Jamaica’s July 2026 outsourcing consultation provides a regional reference for service continuity and oversight. Check the current local rules before signing a contract.[12] [11] [26] [10]

Bank strategy	What AI can improve	How the plan can fail	What to measure
Growth and market entry	Compare customer requests and service gaps across branches.	Incorrect market estimates lead the board to fund a service with little demand.	Paid pilot demand, repeat use and actual service cost.
Credit and pricing	Route straightforward cases and identify file gaps.	Local income patterns produce weak decisions or unequal prices.	Arrears, price gaps and reversals by product and borrower group.
Cost and staffing	Reduce time spent drafting and sorting routine cases.	Rework increases or the bank loses experienced reviewers.	Time to approved work, correction cost and reviewer coverage by shift.
Treasury and capital	Compare cash forecasts and flag gaps in funding.	A shared model misses a rate change or a report omits a large balance.	Forecast error, same-day cash headroom and losses under a common shock.
Customer service	Answer routine questions in more than one language.	A tool gives a wrong deadline or blocks access to a person.	Disputes that miss deadlines, repeat calls and errors by language.
Fraud and cyber defence	Group alerts and help staff find related cases.	Staff miss fraud when the tool hides weak alerts. An agent can expose records if it has excess access.	Missed losses, response time and actions beyond approved permissions.
Partnerships and outsourcing	Buy a service the bank cannot build quickly.	Several providers depend on the same host or technical team.	Time to recover on an independent service and the cost to leave.

Bank strategy	What AI can improve	How the plan can fail	What to measure
Infrastructure lending	Finance projects with proven tenants and durable contracts.	Several loans rely on one buyer, grid or technology. New AI can reduce demand for current equipment.	Exposure by shared tenant, drawn credit and recovery value under stress.
Data policy and local capability	Keep control of records and test services on local products.	A deadline forces a weak local service into use. The fallback shares its failure point.	Pass rates by product and country, independent restoration and trained staff per shift.

What boards can ask for

Risk teams can use the register to assign owners and select tests. Start with shared suppliers, services that move money and reports that determine cash or capital. Each affected team must know who can stop the AI system and which service takes over.

Ask Treasury to rehearse a run on deposits when mobile banking is down. Ask the payments team to prove that an urgent transfer still requires two authorised people. Ask Credit to compare loan decisions across the groups it serves. Record the failed tests and the date of the next rehearsal.[10] [4] [9]

Use bank records to replace the exercise inputs. Keep the number of cases reviewed, the number of errors that passed the checks and the cost of recovery. Keep near misses that involved an outage or a shared supplier. Track how long it took for harm to reach other teams, customers or banks. Re-estimate after a change in volume, autonomy, supplier or control. Retain the previous estimate and its date.

Sources

• Bank of England and Financial Conduct Authority (2024). Artificial intelligence in UK financial services.

• Bank of England and Financial Conduct Authority (2026). Artificial intelligence in UK financial services.

• Financial Stability Board (2024). The financial stability implications of artificial intelligence.

• Financial Stability Board (2025). Monitoring adoption of artificial intelligence and related vulnerabilities in the financial sector.

• International Monetary Fund (2024). Global Financial Stability Report, October, chapter 3. AI in capital markets.

• International Monetary Fund (2024). Global Financial Stability Report, April, chapter 3. Cyber risk and financial stability.

• International Monetary Fund (2026). Global Financial Stability Report, October.

• Bank of England (2026). Financial Stability Report, July.

• Federal Reserve, Office of the Comptroller of the Currency and Federal Deposit Insurance Corporation (2026). Revised guidance on model risk management.

• Basel Committee on Banking Supervision. Consolidated banking guidelines on operational resilience.

• Bank of Jamaica (2026). Consultation draft on outsourcing and third-party risk management.

• World Bank (2025). Digital Progress and Trends Report. Strengthening AI Foundations.

• Dell’Acqua et al. (2023). Navigating the Jagged Technological Frontier. Working paper.

• BetterUp Labs and Stanford Social Media Lab (2025). US desk-worker survey on workslop.

• Bartlett, Morse, Stanton and Wallace (2022). Consumer-lending discrimination in the FinTech Era. Journal of Financial Economics.

• Consumer Financial Protection Bureau (2023). Chatbots in consumer finance.

• Financial Crimes Enforcement Network (2024). Alert on deepfake fraud targeting financial institutions.

• Hong Kong Government (2024). Legislative Council reply on fraud involving deepfakes.

• US Securities and Exchange Commission (2013). Administrative order concerning Knight Capital Americas.

• Federal Reserve (2023). Review of the Federal Reserve's supervision and regulation of Silicon Valley Bank.

• CrowdStrike (2024). Form 8-K on the 19 July update and outages.

• Federal Deposit Insurance Corporation. Failed bank list for the United States.

• Banco Popular Dominicano (2025). Notice on a fake video of its chief executive.

• Bank of Jamaica (2026). Financial Policy Committee statement, November.

• Bank of Jamaica (2026). Statement on the cyber incident at JETS Limited.

• UNESCO. Caribbean Artificial Intelligence Policy Roadmap.

About the author

Adrian Dunkley is an AI expert, an experienced C-suite banker and an investor.