



CMCS INSIGHTS · OWNERS · GOVERNANCE & AUDIT

Project Fraud Prevention with PMWEB

Seven articles on how a PMIS like PMWEB prevents, deters and detects fraud on capital projects: a lifecycle view of fraud risk, authority enforced through workflows and the DoA matrix, procurement integrity, traceable RFIs, change and claims, payment integrity, forensic audit, and how PMWEB 2026 AI and analytics detect fraud patterns across the portfolio.

By Bassam Samman, PMP, PSP, EVP, GPM
CEO & Chairman, CMCS

IN THIS SERIES

7 articles

-
- 01 Project Fraud Starts Where Governance Stops: A Lifecycle View of Fraud Risk on Capital Projects
 - 02 Authority Enforced, Not Assumed: Workflows, the DoA Matrix and Delegation in PMWEB
 - 03 Procurement Integrity: Prequalification, Bid Analysis and Unbalanced Bids in PMWEB
 - 04 Change Without Cover: Tracing RFIs, PCOs, Change Orders and Claims in PMWEB
 - 05 Payment Integrity: Detecting Abuse of Approval Power on Interim Payment Certificates
 - 06 Forensic Audit in PMWEB: Rebuilding the Record to Recover Lost Funds
 - 07 From Red Flags to AI: How PMWEB 2026 and Analytics Detect Fraud Patterns Across the Portfolio
-

Project Fraud Starts Where Governance Stops — A Lifecycle View of Fraud Risk on Capital Projects

From twenty fraud actions to a governance model the system enforces

Fraud on a capital project rarely needs a criminal mastermind. It needs a decision nobody has to justify, a transaction nobody has to evidence, and an approval nobody can trace. When the owner leaves those gaps open, the owner is, in effect, inviting fraud.

Capital projects carry more fraud risk than day-to-day corporate operations. Corporate finance runs on enforced policies, a general ledger and an audit calendar. A project, by contrast, is a temporary organisation of owner staff, consultants, contractors and suppliers, assembled under time pressure, spending large sums through hundreds of contracts and thousands of transactions. Each estimate, bid evaluation, change order, payment certificate and inspection is a decision point. Each decision point is a place where someone can favour a party, hide a delay or move money for personal gain.

Is this article for you?

This series is written for capital project owners, PMOs and project management consultants who believe their projects are digitally controlled, and for those who know they are not. In particular, it is for organisations that:

- **Run delivery through Aconex or another document management system**, where RFIs, variations and payment certificates move as correspondence and attachments.
- **Use a CDE whose workflows review documents** but cannot route a transaction by its value, category and contract impact under a Delegation of Authority matrix.
- **Use a PMIS that cannot integrate with the ERP**, so approved figures are re-keyed into finance and two versions of the truth exist.
- **Use a PMIS without comprehensive cost and contract management**, so estimate, budget, bids, commitments, changes, invoices and payments are not one connected chain.
- **Fund or invest in capital projects as a ministry of finance or sovereign fund**, and need assurance that the capital provided is spent on verified delivery.
- **Advise clients on project governance as management consultants**, and want recommendations that are enforced by a system rather than bypassed in practice.
- **Use no system at all**, relying on email, paper and spreadsheets.

Each part shows, process by process, where these set-ups leave the fraud risk open, how PMWEB closes it, and why organisations on the wrong platform have no excuse left for not migrating.

The Association of Certified Fraud Examiners estimates in its *Occupational Fraud 2024: A Report to the Nations* that organisations lose about 5% of revenue to fraud each year, that a typical scheme runs for a year before it is detected, and that more than half of cases trace back to missing internal controls or managers overriding the controls that exist. Construction ranks among the sectors with the highest median loss per case. On a giga-project portfolio, 5% of annual capital spend is not a rounding error. It is a hospital, a school cluster or a road network that never gets built.

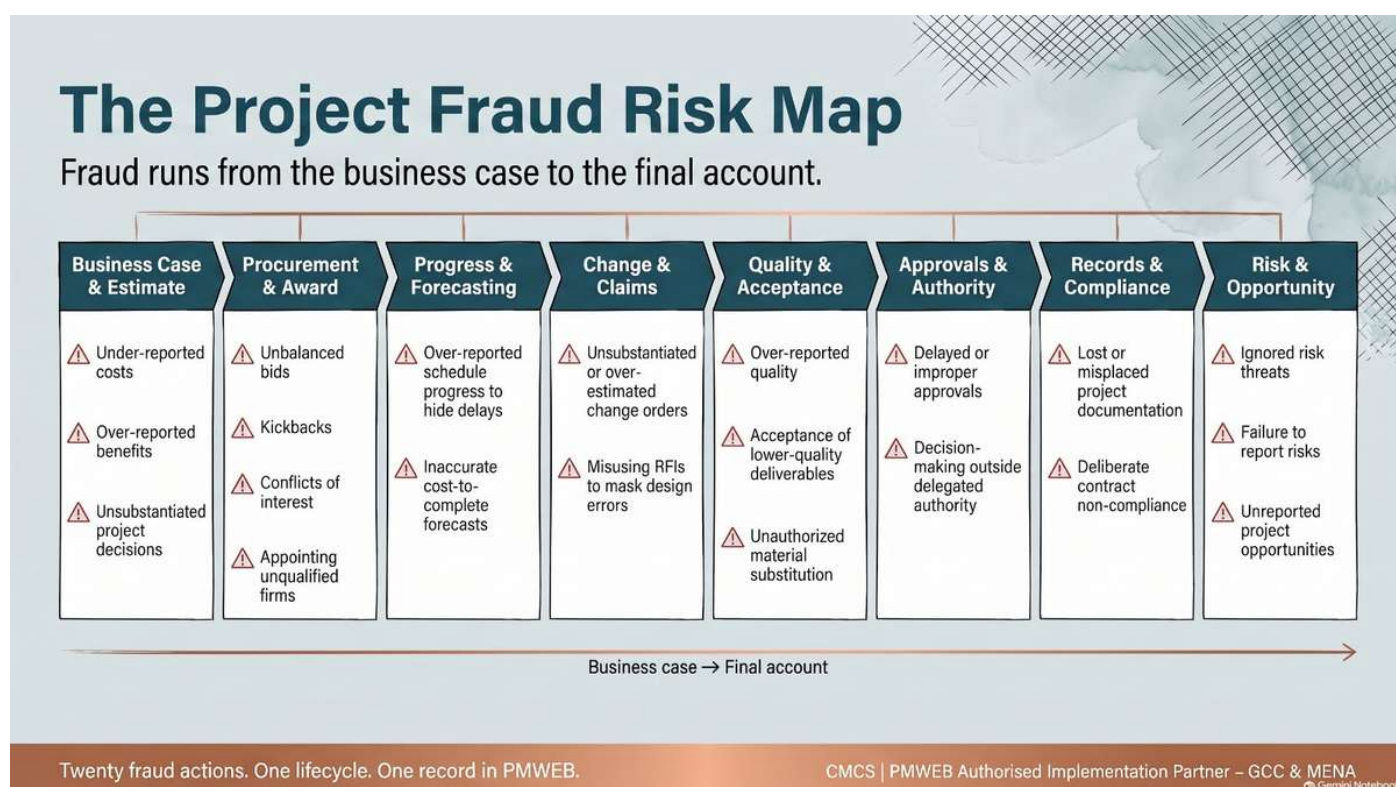
This series rewrites and expands my earlier articles on how a Project Management Information System (PMIS) like PMWEB prevents and detects fraud on capital construction projects. Part 1 sets out the fraud risk across the project lifecycle and the governance model that deters it. Parts 2 to 6 take each high-risk area in turn: approval authority, procurement, change and claims, payments, and forensic audit. Part 7 shows how PMWEB 2026 AI and analytics built on PMWEB data move the owner from finding fraud after the money has gone to flagging it while the transaction is still open. A thread runs through every part: platforms that were never designed as a PMIS, such as document management systems, ERPs, e-tendering portals and generic workflow tools, give owners the false assurance that their projects are digitally controlled when the controls that deter and detect fraud are not there.

What Counts as Project Fraud

Fraud is deceiving someone to obtain an unfair or unlawful gain. On a capital project it takes two forms. The first is the act itself: a kickback, a fake invoice, an inflated change order. The second, far more common, is the decision or report that hides the truth from the owner: an estimate understated to get a project approved, a schedule overstated to hide a delay, a deliverable accepted that was never fit for purpose. Both cost the owner money, time, quality or reputation.

The twenty actions below come from my original article. Grouped by where they happen, they show that fraud is not confined to procurement or payments. It runs from the business case to the final account.

Fraud risk area	Typical fraud actions
Business case and estimate	Unsubstantiated project decisions; under-reported cost estimates; over-reported benefits
Procurement and award	Unbalanced bids; conflict of interest and kickbacks; appointing unqualified firms or team members
Progress and forecasting	Over-reported schedule progress to hide delays; wrong forecasts of the cost to complete
Change and claims	Unsubstantiated change orders; over-estimated change orders; misuse of RFIs to cover design errors
Quality and acceptance	Over-reported quality progress; acceptance of lower-quality deliverables; substitution of specified materials
Approvals and authority	Delayed or improper approvals; decisions outside delegated authority; intended wrong actions or decisions
Records and compliance	Lost or misplaced project documents; non-compliance with contract terms; negligence in protecting the owner's interest
Risk and opportunity	Creating avoidable threats by ignoring best practice; failing to report threats or opportunities in time



The Risk Everyone Knows and Nobody Names

Every experienced owner, consultant and contractor knows that fraud happens on capital projects. Ask privately and most can describe a case. Yet project fraud rarely appears in a risk register, a board paper or a project review. It is spoken about as something that happens on other projects, in other organisations, in other countries.

The silence has understandable causes. Naming fraud feels like accusing colleagues. Executives worry that admitting the risk will be read as admitting failure. Partners and contractors fear losing future work. Public bodies fear headlines. So the risk is managed by hoping, and a risk that cannot be named cannot be measured, owned or reduced.

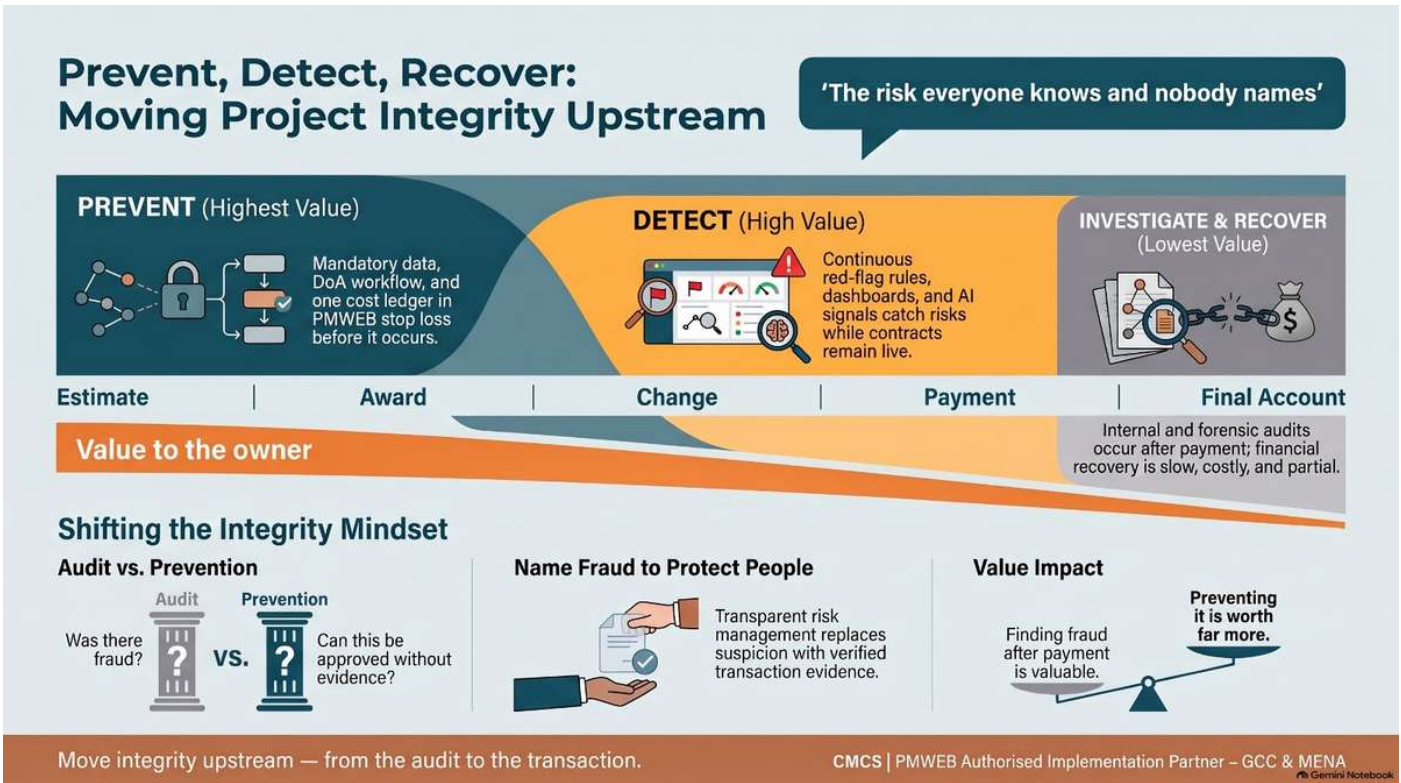
It takes courage for a board or a PMO head to say openly: fraud is a risk on our projects, as it is on every capital programme, and we will manage it like any other risk, with an owner, controls, indicators and reporting. Saying so is not an accusation against anyone. It protects honest people, because it replaces suspicion with evidence.

Audit Finds Fraud; Controls Prevent It

Where fraud is addressed, the main tool is usually audit: internal audit reviews, external audits, state audit bureau inspections, and forensic audits when something has clearly gone wrong. These are essential, but they share one limitation. They look backwards. Audits are periodic, they test samples, and they usually start after the estimate was approved, the contract awarded, the change order signed and the payment made. Their question is "was there fraud?", and if the answer is yes, the money is already gone and recovery is slow, costly and partial.

The ACFE figures above show the cost of that delay: a typical scheme runs for about a year before it is detected. Prevention asks a different and more valuable question: "can this transaction be approved without the evidence, the authority and the checks it needs?" If the system makes the answer no, the fraud never happens.

Line of defence	When it acts	Typical method	Value to the owner
Prevent	Before and during each transaction	Mandatory data, checklists, DoA workflow, segregation of duties, one cost ledger — enforced in PMWEB	Highest: the loss never occurs
Detect	Continuously, every period	Red-flag rules, dashboards and AI signals on PMWEB data	High: exposure is caught while the contract is still live
Investigate and recover	After the event	Internal, external and forensic audit	Lowest: recovery is partial, slow and costly



This series is built on that shift. Audit remains necessary, and Part 6 shows how PMWEB strengthens it. But the controls in Parts 2 to 5 act at the moment of the transaction, and the analytics in Part 7 act continuously, so the auditor's job changes from finding fraud after the fact to confirming that the controls work.

Why Owners Unintentionally Encourage Fraud

In most fraud investigations I have seen, the policies existed. The procedures manual existed. What did not exist was a way to make every person follow them every time and to prove afterwards who did what. The conditions that encourage fraud are predictable:

- **No stated policy.** Without an explicit zero-tolerance policy, fraud is treated as a disciplinary matter for individuals rather than a risk the organisation manages.
- **Procedures on paper only.** The standard operating procedures manual defines forms, workflows and authority levels, but nothing stops a transaction from skipping them.
- **Data silos.** Estimates sit in spreadsheets, contracts in a shared drive, invoices in finance, correspondence in email. Each reconciliation is manual, and every manual step is a place where numbers can be adjusted.
- **Financial ambiguity.** Budget, commitments, pending and approved changes, invoices and payments are never seen together, so an over-commitment or a duplicated payment is invisible.
- **No record of decisions.** When decisions are made in meetings and emails, nobody can later show who decided, on what evidence and under which authority.
- **Resistance dressed as practicality.** "The contractor will not enter data" and "the system slows us down" are common objections. Sometimes they are genuine. Sometimes the objection is to transparency itself.
- **Digitalisation in name only.** Documents, payments and tenders run on platforms that were never designed as a PMIS, so management believes controls exist that do not.

The Most Dangerous Control Is the One You Think You Have

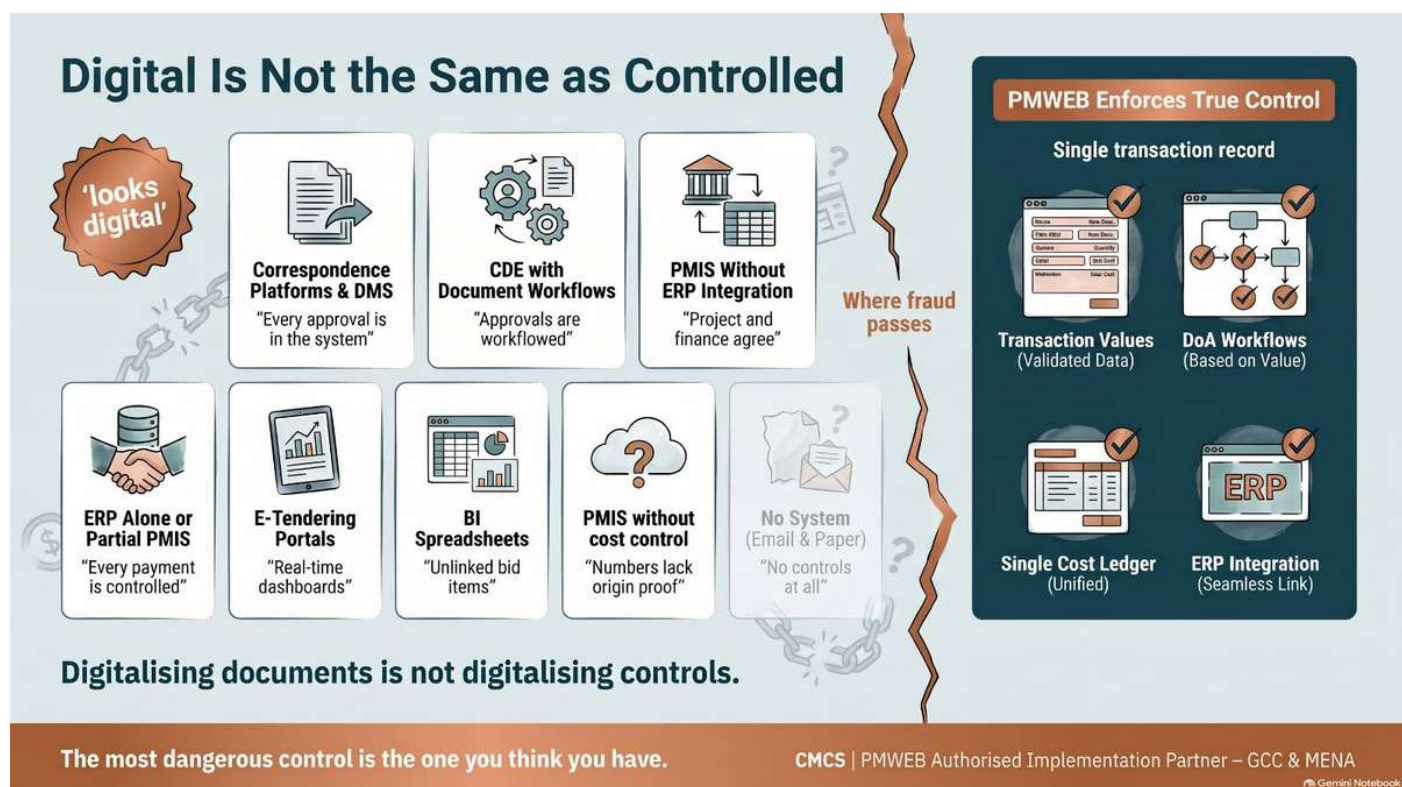
Many owners will read the section above and conclude that the problem is solved, because their projects are already "digital". Drawings and correspondence go through a document management system or common data environment. Purchase orders and payments go through the ERP. Tenders are issued on an e-tendering portal. Approvals are routed through a generic workflow or low-code tool. Monthly reports are built from spreadsheets with a business intelligence layer on top.

Each of these tools is good at the job it was designed for. None of them was designed to manage the business processes of capital project delivery. The same applies to some products sold as a PMIS: if the system cannot be integrated with the ERP, or does not cover cost and contract management from estimate to payment, the most fraud-exposed transactions still sit outside it. Used in place of a PMIS, they do something worse than leave a gap: they create **false assurance**. The board, the auditors and the regulators are told that the projects are digitalised, so they assume that the controls a digital system should provide are in place. They are not. Fraud then runs through the gap between what the organisation believes is controlled and what is actually controlled.

Platform used as a PMIS	What it was designed for	What it cannot do for fraud control	The false assurance it creates
Correspondence-centric platform such as Aconex, or a document management system	Controlling, transmitting and tracking correspondence, documents and drawings	Read the amounts, causes and quantities inside the PDF; route by transaction value; link an RFI's cost impact to a commitment	"Every letter and approval is in the system"
ERP	Accounting, purchasing and payment after a commitment exists	See estimates, bid line items, pending changes, PCOs, claims, work in place or inspections	"Every payment is controlled in the ERP"
E-tendering portal	Issuing tenders and receiving submissions securely	Compare bid line items with the approved estimate; carry evaluated rates into the contract and its changes	"Procurement is online and transparent"
CDE with document-review workflows	Sharing and approving information containers and models	Route a change order or invoice by value, category and contract impact under the DoA; hold the approved amount as data	"Our approvals are workflowed"
PMIS without ERP integration	Managing project processes in isolation	Pass approved commitments, certificates and payments to finance without re-keying, or reconcile the two	"Project and finance figures agree"

Platform used as a PMIS	What it was designed for	What it cannot do for fraud control	The false assurance it creates
PMIS without full cost and contract management	Scheduling, field or document processes	Connect estimate, budget, bids, commitments, PCOs, change orders, invoices and payments in one cost ledger	"We have a PMIS"
Generic workflow or low-code tool	Routing forms and tasks of any kind	Hold a cost ledger, contract schedule of values or DoA logic tied to commitments; survive staff turnover of the people who built it	"Approvals are automated"
Spreadsheets with a BI layer	Analysis and presentation	Prove where a number came from, who changed it and who approved it	"We have real-time dashboards"
No system: email, paper and spreadsheets	Nothing in particular	Any of the above	None, but also no controls

The pattern is the same in every case. The tool records that a **document** was uploaded, viewed, stamped or sent. A PMIS records that a **transaction** was submitted, checked, approved within authority and posted to the cost ledger, with every value held as data. Fraud is committed in the transaction, not in the file name. A system that cannot read the transaction cannot test it.



Six questions to test whether your digitalisation deters fraud

1. Can the system tell you the approved budget, committed value, pending changes, approved changes, work in place, invoiced and paid for any contract, today, without a spreadsheet?
2. Does the system decide who approves a change order or invoice from its value and contract impact, or does a person choose the reviewers?
3. Can the system compare every bid line item with the approved estimate, and every change order rate with the contract rate?
4. If a change order is approved in a document platform, can anyone prove the figure paid in the ERP is the figure that was approved?
5. Could an auditor run the red-flag rules in this article on your data, or would they first have to rebuild it from PDFs?

6. Do the figures approved in your project system reach the ERP through integration, or are they keyed in again by someone in finance?

If the honest answer to any of these is no, the organisation has digitalised its documents, not its controls. The rest of this series shows, process by process, where that difference lets fraud through.

Time to Move: Migrating to a PMIS Like PMWEB

If the six questions above show that an organisation's fraud-exposed processes run on the wrong platform, the recommendation is direct: it should migrate them to a PMIS like PMWEB. Today there is no credible excuse for continuing to run them where they are. Adding another policy, another review step or another spreadsheet to a platform that cannot read the transaction will not close the gap. It will only deepen the false assurance.

Organisations often delay migration because the current platform is familiar, contracts with suppliers are in place, and moving project information feels risky. Those concerns are real, but they need to be weighed against the cost of staying. Every year on a platform that cannot enforce the DoA, compare bids with the estimate, link change to its cause or reconcile certificates to payments is a year of exposure to the leakage priced in the ROI section below. On a large capital programme, the cost of staying usually exceeds the cost of moving within the first year.

If you are on...	What to keep	What to move to PMWEB	How the transition works
Aconex or another document management system	Correspondence and document control during transition, if required	RFIs, change events, PCOs, change orders, claims, commitments, progress invoices, budgets and approvals	PMWEB integrates with Aconex; CMCS also migrates project data from Oracle Aconex and Oracle Unifier to PMWEB
A CDE without DoA-driven workflows	Models, drawings and information containers in the CDE	Every transaction that changes cost, time or contract, with DoA workflow and the cost ledger	PMWEB integrates with Autodesk ACC, SharePoint and Egnyte, and with other DMS platforms by configuration
A PMIS without ERP integration	The ERP as the financial book of record	Project cost and contract processes, integrated with the ERP through PMWEB's open APIs	Approved commitments, certificates and payments pass between systems without re-keying
A PMIS without full cost and contract management	Any specialist tools that integrate with PMWEB, such as Primavera P6	The estimate-to-payment chain: estimate, budget, bids, commitments, changes, invoices, payments	Run PMWEB as the system of record for cost and contract, linked to the schedule
No system: email, paper and spreadsheets	Nothing that cannot be evidenced	All delivery processes, starting with procurement, change and payment	Start PMWEB on a new programme and expand

A low-risk migration path

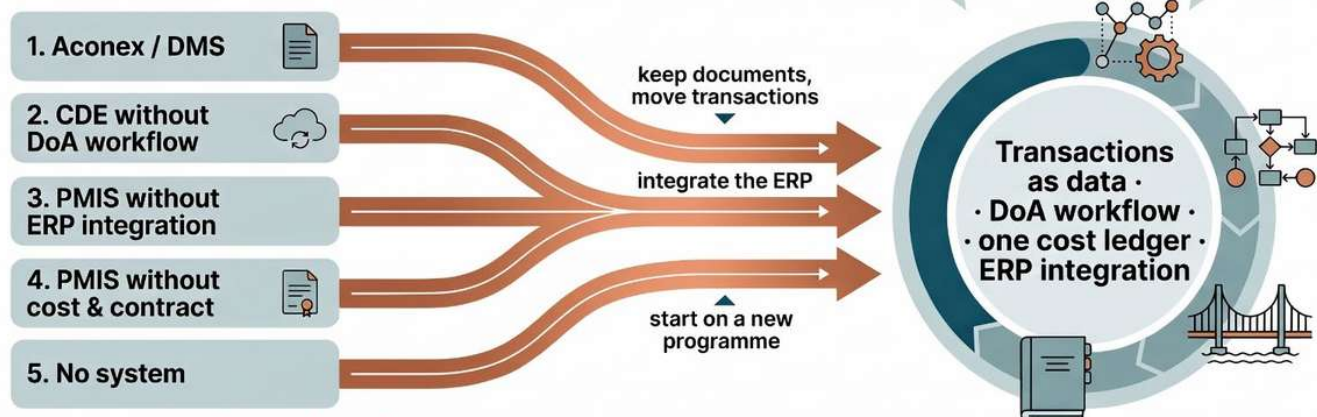
1. **Assess.** Map which processes run where, and how legacy data is held: its structure, media, size and consistency across projects. That assessment decides what is migrated and what is archived.
2. **Start where risk is highest.** Move procurement, change and payment processes first, because that is where fraud exposure and value are concentrated.
3. **Start on a new programme.** A PMIS is programme-scoped, so PMWEB can go live on a new programme while existing projects continue on the current platform, avoiding a big-bang cut-over.
4. **Configure, do not code.** PMWEB is configured to the organisation's procedures, DoA matrix and forms, which keeps the implementation fast and the system owned by the client.
5. **Integrate rather than duplicate.** Connect the ERP and any document platform that remains, so each transaction is entered once.
6. **Migrate live projects in waves.** Bring the cost and contract records of ongoing projects into PMWEB in planned waves; PMWEB's Microsoft SQL Server database makes structured data loading and validation straightforward.
7. **Close the back door.** Once a process runs in PMWEB, stop accepting off-system approvals for it.

No excuse left

The reasons given for staying on the wrong platform are familiar. None of them survives contact with the facts, and every month of delay is paid for in exposure.

The excuse	The reality
"We already have a system."	A system that cannot read the transaction does not control it. That is false assurance, and it is worse than knowing you have no control.
"Migration is too risky."	PMWEB starts on a new programme and takes live projects across in planned waves. There is no big-bang cut-over. The real risk is continuing as you are.
"It will take years."	PMWEB is configured, not coded, and is implemented in months, starting with the highest-risk processes.
"It is too expensive."	Avoiding a fraction of one percent of leakage repays the system many times over every year. The expensive option is staying.
"We would waste our investment in Aconex, our DMS or our CDE."	PMWEB integrates with Aconex, Autodesk ACC, SharePoint and Egnyte. Keep the document platform for documents; move the transactions.
"Our ERP already controls payments."	The ERP controls the payment run, not the certificate behind it. PMWEB integrates with the ERP so both hold the same approved figures.
"Contractors and consultants will not enter data."	Making submission through the PMIS a contractual requirement is a governance decision. Resistance to transparency is itself a red flag.
"Our team cannot maintain a PMIS."	PMWEB is configured by the owner's own team or its consultants and owned by the client, not locked to a supplier.
"We will wait for AI."	AI cannot detect fraud in transactions that are not captured as data. Migration is the prerequisite for AI, not an alternative to it.

Migration Paths to PMWEB — No Excuse Left



The cost of staying is the leakage — every year.



No excuse to stay on the wrong platform.

CMCS | PMWEB Authorised Implementation Partner – GCC & MENA

The Governance Model That Deters Fraud

My original article set out four pillars. They remain valid, with one change: the enabler is no longer optional. Without a system that enforces the method, the objective stays a statement on the wall.

Pillar	What it means	How PMWEB makes it real
Objective	A clear zero-tolerance policy on project fraud, approved by the board	Policy published in the PMWEB document repository; integrity red flags tracked as records with owners and due dates
Method	A standard operating procedures manual: organisation, lifecycle stages and gates, processes, forms, DoA matrix and process KPIs	Each procedure configured as a PMWEB template, workflow and report, so the manual is executed rather than read
Enabler	An integrated PMIS that captures every transaction, document and approval in one database	One platform for estimate, budget, procurement, contracts, changes, invoices, payments, quality and documents
Commitment	Top management names fraud openly as a risk, sponsors the controls and applies consequences for non-compliance	Executive dashboards show compliance, exceptions and open red flags; nothing is approved off-system

Organisation, lifecycle and stage gates

The procedures manual starts with the organisation that manages the portfolio, whether a projects department, project management unit or PMO, with its roles and responsibilities. It then defines the lifecycle from planning and concept design through detailed design, procurement, construction and defects liability, with a stage gate between each stage at which the owner decides whether the project proceeds. In PMWEB each gate is a record with its own checklist, evidence and approval workflow, so no project can pass a gate on a verbal assurance.



The processes that need the tightest control

The manual typically covers twenty or more procedures. The ones with the highest fraud exposure, and the PMWEB modules that hold them, are:

Procedure	PMWEB module or form	What the record captures
Project approval and budgeting	Cost estimate, budget, budget requests	Approved estimate, baseline budget, every transfer with requester, approver and reason
Prequalification of consultants, contractors and suppliers	Vendor prequalification	Scored qualification, financial capacity, track record, conflict-of-interest declarations

Procedure	PMWEB module or form	What the record captures
Bid packages and procurement	Procurement / bid packages	Invited bidders, bid line items against estimate, technical scores, recommendation
Agreements and contract authorisation	Commitments	Contract value, schedule of values, retention, terms and clauses
Design and construction changes	Change events, PCOs, change orders	Cause, linked RFI, cost and time impact, line items, approvals
Payment applications	Progress invoices, payments	Work in place, stored materials, retention, approved and paid amounts, dates
Submittals, inspections and NCRs	Submittals, WIR/MIR and NCR forms	Specified versus submitted, inspection checklists, non-conformances and closure
Delays, time extensions and liquidated damages	Schedule, claims and EOT forms	Entitlement, affected activities, assessed time and cost
Taking over and closeout	Punch lists, closeout forms	Snags, certificates, final account, lessons learned

The screenshot displays the PMWEB application interface. On the left is a dark sidebar menu with icons and labels for various sections: Plans, Forms, Costs, Schedules, Assets, Workflows, Portfolio, Tools, Recent Records, Search, and PMWEB University. The main content area is divided into three columns under the heading 'Costs'. The first column lists categories like Budgets, Funding, Contracts, and Change Management. The second column lists specific forms and documents, such as Invoices, Payments, and Advanced Multi-currency. The third column shows a list of records with details like 'Test 12', 'Provisional Sums Tracker', and 'L01 Notice of Not Foreseeable Phys...'. On the right, a detailed form is visible, featuring fields for Location, WBS, Target Revenue, Target Finish, and Workflow Calendar, along with a file upload section.

How PMWEB Turns Procedures Into Controls

Every business process in PMWEB follows the same pattern. Each element closes a specific fraud opportunity.

PMWEB element	What it does	Fraud opportunity it closes
Template	Standard input form with mandatory fields and predefined value lists	Incomplete or selective information; free-text manipulation of categories
Field-level permissions	Only authorised roles can create, edit or view each form and field	Unauthorised edits of values, dates or status
Attachments and links	Supporting documents, linked records and imported emails stored on the record	Claims and approvals made without evidence; lost or substituted documents
Workflow	Review and approval steps, roles, durations and branches tied to the DoA matrix	Approvals by the wrong person, above their limit, or out of sequence

PMWEB element	What it does	Fraud opportunity it closes
Workflow history	Date, time, user, action, comments and delegate for every step	Denial of responsibility; back-dated or undocumented decisions
Cost ledger	Every financial transaction posted automatically to one ledger	Financial ambiguity between budget, commitments, changes, invoices and payments
Reports and dashboards	Logs, output forms and Power BI reports across projects and programmes	Patterns that are invisible in a single transaction

One Version of the Truth Removes Financial Ambiguity

Financial ambiguity is one of the most common enablers of project fraud. When the estimate, budget, bids, awarded contracts, pending and approved changes, invoices, payments and funding releases sit in separate silos, nobody can see that a contract has been over-committed, that the same work has been paid twice or that contingency has been quietly spent. In PMWEB, every one of those transactions posts to the same cost ledger the moment it is approved. The cost worksheet shows them side by side for each cost code, contract and project, and the same data rolls up to programme and portfolio.

The same principle applies beyond cost. Schedule, deliverables, quality, safety and document approvals are captured in the same database, so the executive view of the project is calculated from the transactions rather than reported about them.

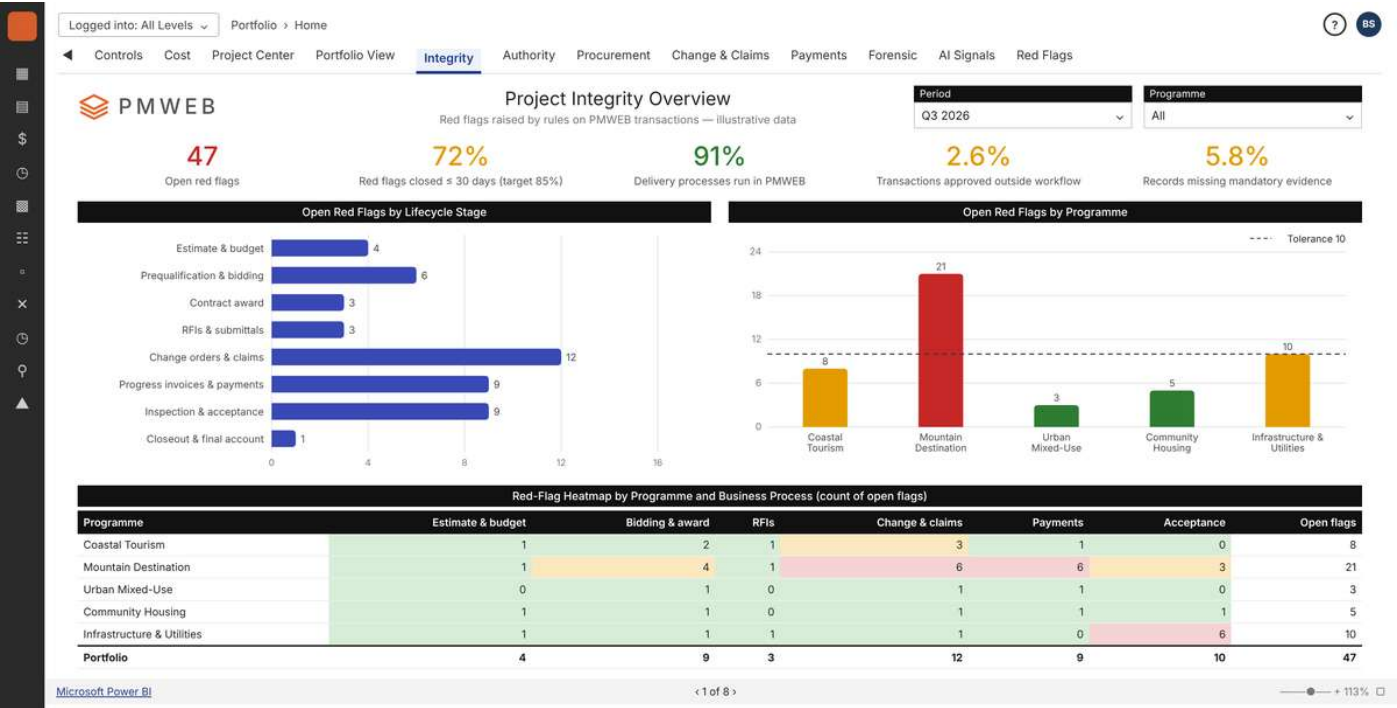
From Controls to Red Flags

Controls prevent most fraud. They do not prevent all of it, because people with legitimate access can still misuse it. The second line of defence is a set of red-flag rules that run on PMWEB data every period. A red flag is a question, not a verdict. It tells the integrity or audit team where to look; the investigation decides whether there was wrongdoing.

Red flag	What it may indicate	PMWEB data used
Award well below the approved estimate	Unbalanced bid or inside knowledge of future changes	Cost estimate, bid comparison, commitments

Red flag	What it may indicate	PMWEB data used
Change ratio rising on one contractor across projects	Claim-oriented contractor or design errors being paid for twice	Change orders, commitments, projects
Invoice approval much slower or faster than the norm	Approval power used to pressure or favour a contractor	Progress invoice workflow history
Approver also the submitter, or above DoA limit	Control override	Workflow history, DoA rules
Progress claimed ahead of accepted inspections	Over-reported progress or payment for work not done	Progress invoices, WIR records
Records without mandatory evidence	Lost, withheld or substituted documents	Attachments, completeness queries

Each flag raised becomes an *Integrity Red Flag* record in PMWEB, created as an adaptive form linked to the source transaction, with a severity, an owner, a due date, the evidence attached and a workflow that routes it to the integrity or internal audit function. The flag itself is then auditable: who reviewed it, what they found and how it was closed.



Project Integrity Overview — a Power BI report on the PMWEB database, embedded in PMWEB. Illustrative data for a five-programme giga-developer portfolio.

The integrity overview shows open red flags by lifecycle stage and by programme, and a heatmap of programme against business process. In the illustrative data, the portfolio total of 47 open flags looks manageable until the heatmap shows that 21 of them sit in one programme, concentrated in change orders and payments. That is where the integrity team starts. Every number opens to the flags behind it, and every flag opens to the PMWEB record that triggered it.

Where PMWEB 2026 AI Helps

Part 7 covers AI in depth. Even at this stage, the PMWEB 2026 AI Assistant changes how a reviewer works with the data. It can **find** records in plain language ("show me change orders over SAR 1 million on the Mountain Destination programme approved in under three days"), **open** them, **create** records such as a red flag with the user's approval, and **help** users understand a process or a screen. It acts only with the user's approval and honours PMWEB security settings, so a reviewer sees only what their role allows. The value of any AI rests on the same foundation as the controls in this article: complete, structured, approved transaction data in one database.

Paper, Non-PMIS Platforms and PMWEB Compared

Capability	Procedures manual alone	Document platform, ERP or generic workflow	Procedures enforced in PMWEB
Forms	Word and Excel templates, filled differently by each team	PDFs or generic e-forms; values held as text, not validated data	Standard templates with mandatory fields and value lists
Approvals	Signatures collected by email or on paper	Document stamps or generic flows with no DoA logic on transaction value	Workflow with DoA rules, delegation and a full history
Evidence	Scattered across drives and inboxes	Stored, but not tied to the transaction it supports	Attached and linked to each record
Financial view	Reconciled by hand each month	ERP shows committed and paid, not pending changes or work in place	One cost ledger, updated on approval
Exceptions	Found by auditors months later, if at all	Invisible, because the data the rules need is never captured	Flagged by rules every period
Accountability	Disputed after the event	Shows who opened or stamped a file, not who approved what amount	Recorded at the time of each action

The ROI of a PMIS When Fraud Is Priced In

Business cases for a PMIS are usually built on productivity: fewer manual reports, faster approvals, less time reconciling spreadsheets. Those benefits are real, but they are the smaller part of the return. The larger part is the loss that does not happen. Because fraud is rarely named as a risk, it is rarely counted as a benefit, and the business case understates the value of the system by an order of magnitude.

The arithmetic is simple. The ACFE's cross-industry estimate is that organisations lose about 5% of revenue to fraud. Capital programmes are not the same as corporate revenue, so assume something far more conservative: that a PMIS which enforces the controls in this series reduces fraud-related leakage by only a fraction of one percent of annual capital spend. The table shows what that is worth each year.

Annual capital spend ↓ Leakage avoided →	0.25%	0.5%	1%	2%
SAR 1 billion	SAR 2.5m	SAR 5m	SAR 10m	SAR 20m
SAR 5 billion	SAR 12.5m	SAR 25m	SAR 50m	SAR 100m
SAR 20 billion	SAR 50m	SAR 100m	SAR 200m	SAR 400m

Illustrative arithmetic, not a forecast. Each owner should apply its own capital spend and its own view of exposure.

Set any of those figures against the full cost of owning and implementing a PMIS across the same portfolio, and the return is measured in multiples, not percentages. On a giga-project portfolio, avoiding a quarter of one percent of leakage alone can repay the system many times over every year, before a single productivity benefit is counted.

Fraud prevention also carries returns that never appear as a line item:

- **Claims avoided.** Fair, fast and evidenced payment and change decisions remove the grievances that turn into claims and disputes.
- **Lower audit and investigation cost.** Auditors test controls and evidence already in the system instead of rebuilding records.
- **Faster recovery when something does go wrong.** The evidence chain exists from the first transaction.
- **Confidence of funders and stakeholders.** Boards, ministries of finance, lenders and investors rely on figures that can be traced to approved transactions.
- **Deterrence.** The most valuable control is the one that stops an attempt before it is made. Its return is real even though no report will ever show the fraud that never happened.

The ROI of a PMIS When Fraud Is Priced In

Example: avoiding 0.5% leakage on SAR 5bn a year = SAR 25m every year



Price fraud into the business case and a PMIS repays itself many times over.

The cheapest loss is the one that never happens.

CMCS | PMWEB Authorised Implementation Partner – GCC & MENA

For Ministries of Finance and Sovereign Funds: Protecting the Capital You Provide

Ministries of finance appropriate and release the capital that government entities spend on projects. Sovereign funds invest it, as equity in giga developers, project companies and public-private partnerships, and expect it to be preserved and to earn a return. Both are the parties most exposed to project fraud and the furthest from where it happens. They do not approve change orders or certify payments. They see what the implementing entity or portfolio company reports, usually as periodic summaries assembled from the very tools this series has shown to be fragile.

Every riyal or dirham lost to fraud is capital the ministry must find again, or a return the fund will never earn. Under the illustrative arithmetic in this article, avoiding even a quarter of one percent of leakage across a national capital programme or an investment portfolio is worth tens or hundreds of millions each year. Funders are therefore not only beneficiaries of fraud controls; they are in the strongest position to require them.

Funder's question	What a report alone shows	What PMWEB data lets the funder verify
Is capital being spent on what was approved?	Spend against budget, as reported	Spend traced from budget to commitments, approved changes, certified work and payment, by project and funding source
Are we paying for work actually done?	Percent complete, as reported	Certified amounts by line item, linked to accepted inspections, with approval dates and approvers
Is the entity's governance working?	A statement that procedures exist	DoA compliance, off-system approvals, open red flags and their dispositions
Where is value leaking?	Overruns explained after the event	Change ratio, design-error changes, award-versus-estimate and payment-treatment indicators, by programme
Can the figures be trusted?	Signed management representation	Every figure traceable to an approved transaction and reconciled to the ERP

Conditions funders can attach

- **Funding release against evidence.** Release tranches against certified progress and approved commitments in a PMIS, not against requests supported by spreadsheets.

- **System-enforced governance as a funding or investment condition.** Require implementing entities and portfolio companies to run procurement, change and payment processes in an integrated PMIS with DoA workflow and ERP integration.
- **Funder dashboards from the source.** Receive portfolio dashboards calculated from transaction data, with drill-down rights, instead of periodic reports.
- **Integrity reporting.** Require red-flag indicators and their dispositions to be reported each period, alongside cost and schedule.
- **Consistency across entities.** Apply the same process templates and KPI definitions across all funded entities, so performance and risk can be compared like for like.

For Management Consultants Advising on Project Governance

Management consultants are often the people who define a client's project governance: the PMO operating model, the lifecycle and stage gates, the Delegation of Authority matrix, the policies and procedures, the KPIs. The quality of that work is rarely the problem. The problem is what happens after the report is accepted. If the recommendations are implemented on email, on a document platform such as Aconex, on a CDE with document-review workflows, or on a PMIS that cannot carry cost and contract processes or connect to the ERP, the governance exists on paper and is bypassed in practice. When a fraud case later surfaces, the question asked is whether the governance was adequate, and the adviser's name is on it.

Governance advice is only as strong as its enforcement. The most valuable thing an adviser can add to a governance recommendation is the specification of the system capabilities that make it enforceable, and a way to test that they are in place.

Governance recommendation	System capability required to enforce it	How to test it
Delegation of Authority matrix	Workflow branch rules that read transaction value, category and contract impact; formal delegation with scope and period	Submit a test change order above a threshold and confirm it routes to the right authority
Segregation of duties	Submitter excluded from approval steps; field-level permissions	Attempt to approve a transaction you submitted
Stage-gate approvals	Gate records with checklists, evidence and workflow	Try to pass a gate with an incomplete checklist
Single source of financial truth	One cost ledger fed by estimate, budget, commitments, changes, invoices and payments; ERP integration	Reconcile a contract's approved certificate to the ERP payment without a spreadsheet
Procurement integrity policy	Prequalification scoring, bid line items compared with the approved estimate, bid-to-commitment carry-over	Show line-item bid ratios for the last award
Change control procedure	Linked RFI, change event, PCO, change order and claim records with causes as data	Trace a change order back to its cause and forward to its payment
Fraud risk management	Red-flag rules, an Integrity Red Flag record with dispositions, portfolio dashboards	List open flags with owner, age and disposition

A five-level maturity model for fraud-resistant project governance

Level	Description	Fraud exposure	Typical set-up
1. Informal	Governance is custom and practice; approvals by email and signature	Very high	No system; email, paper, spreadsheets
2. Documented	Policies, SOPs and DoA exist but are not enforced by any system	High	Procedures manual plus spreadsheets
3. Digitised documents	Documents and correspondence are controlled; transactions are still PDFs	High, with false assurance	Aconex, DMS or CDE with document-review workflows; ERP for payments

Level	Description	Fraud exposure	Typical set-up
4. Integrated PMIS	Cost and contract processes run as data with DoA workflow, one cost ledger and ERP integration	Low	PMWEB covering estimate to payment, integrated with the ERP
5. Continuously monitored	Red-flag rules, AI-assisted review and learning analytics on the same data	Lowest, and falling	PMWEB with dashboards, PMWEB 2026 AI and analytics

Level 3 is where many clients sit, and it is the most dangerous level for an adviser to leave them at, because it looks like progress. Moving a client from level 3 to level 4 is usually the single highest-value recommendation in a governance engagement.



The funder's lens — ministries of finance and sovereign funds

- Treat fraud prevention as capital preservation: every loss avoided is capital the ministry does not have to re-appropriate, or a return the fund does not lose.
- Use the maturity model to assess each implementing entity or portfolio company, and set a target level as a condition of funding or investment.
- Ask for dashboards calculated from transactions, not summaries assembled from documents.

Adviser's checklist — for consultants recommending project governance

Questions to ask in the diagnostic

- Is project fraud named in the client's risk register, with an owner, controls and indicators?
- Which of the eight set-ups in this article does the client actually run on, process by process?
- Which governance recommendations from previous reviews are enforced by a system, and which rely on people?
- Where on the five-level maturity model is the client today?

Recommendations to put in the governance report

- Name project fraud as a managed enterprise risk and assign it an owner.

- Specify the system capabilities required to enforce each governance recommendation, using the traceability table.
- Move the most fraud-exposed processes (procurement, change, payment) to an integrated PMIS before refining policy further.
- Report fraud-control effectiveness to the board using the indicators at the end of this article.

Evidence That the Governance Model Is Working

- **Process coverage.** The share of in-scope delivery processes run end to end in PMWEB, with no off-system approvals.
- **Evidence completeness.** The share of records with all mandatory attachments and linked records.
- **Exception rate.** Transactions approved outside workflow or outside the DoA, trending to zero.
- **Red-flag closure.** Flags closed with a documented disposition within the target period.
- **Recurrence.** Repeat flags on the same party or process falling after corrective action.

Key takeaway

Fraud thrives where decisions are undocumented, data is fragmented and approvals are untraceable. A zero-tolerance policy and a procedures manual define what should happen. PMWEB makes it happen, every time, and records who did what, when and on what evidence.

Digitalising documents is not digitalising controls. A platform that was never designed as a PMIS gives the board the comfort of a digital system without the controls of one, and that false assurance is itself a fraud risk.

With every transaction in one database, the owner can move from reacting to fraud after the money has gone to flagging the patterns that precede it.

Project fraud is a known risk that too few organisations have the courage to name. Audit will always find some of it after the money has gone; controls in PMWEB prevent it at the transaction, which is where the real value lies.

Priced against the fraud risk it removes, a PMIS is not a cost to be justified; it is one of the highest-return investments a capital programme can make.

Organisations running their fraud-exposed processes on the wrong platform have no excuse left. They should migrate to a PMIS like PMWEB; the cost of staying is the leakage, every year.

Next in the series: Part 2 looks at approval authority: how PMWEB workflows enforce the Delegation of Authority matrix, handle delegation during absences, and produce output forms that show exactly who reviewed and approved each transaction.

Talk to us: If your projects run on Aconex or another document management system, a CDE without DoA-driven workflows, a PMIS without ERP integration or full cost and contract management, or no system at all, there is no longer an excuse to stay: migrate your fraud-exposed processes to a PMIS like PMWEB. CMCS can assess your current platforms and data, start PMWEB on a new programme, integrate it with your ERP and document platforms, and migrate legacy project data, including from Oracle Aconex and Oracle Unifier. Contact CMCS at info@CMCS-MENA.com. Management consultants designing project governance for their clients are welcome to use these frameworks; CMCS works alongside consulting firms to turn governance recommendations into configured PMWEB processes. Ministries of finance and sovereign funds can also see how a common PMWEB standard across funded entities gives them verified, portfolio-wide visibility.

#PMWEB #CMCS #FraudPrevention #ProjectGovernance #PMO #CapitalProjects #ProjectControls #PMIS #GigaProjects #Integrity #CDE #DocumentManagement #ERPIntegration #ManagementConsulting #MinistryOfFinance #SovereignWealthFund

About the Author

Bassam Samman, PMP, PSP, EVP, GPM is the Chairman and Chief Executive Officer of CMCS FZCO, the PMWEB Authorised Implementation Partner for the Gulf Cooperation Council and broader Middle East and North Africa region. CMCS holds the PMWEB Global Partner of the Year 2025 designation and serves capital project owners, contractors and consultants across the UAE, Saudi Arabia, Qatar and Kuwait.

Bassam has over four decades of experience providing project management, project controls services and project management information systems to more than two hundred capital projects with a combined value exceeding one hundred billion US dollars. He is the author of four published books on project management digitalisation, and has lectured at more than three hundred and fifty international events. He is a co-founder of the Project Management Institute Arabian Gulf Chapter. He holds a Master's degree in Engineering Administration (Construction Management), with Faculty Commendation, from George Washington University and a Bachelor's degree in Civil Engineering from Kuwait University, with executive education at Harvard Business School and London Business School.

About PMWEB

PMWEB is an enterprise-class, web-based capital construction project management platform trusted by organisations worldwide including Harvard University, the United Nations, and Atlanta Airport. Built on Microsoft .NET technology, PMWEB manages the entire project lifecycle within a single integrated platform — from portfolio planning and cost management through document control, procurement, scheduling, asset management, and business intelligence. With 150+ pre-configured SSRS reports, drag-and-drop dashboard design, multi-currency support, and open REST/SOAP API integration, PMWEB delivers enterprise capability with implementation timelines measured in months, not years.

About CMCS

CMCS (Collaboration, Management and Control Solutions) is the PMWEB Authorised Implementation Partner for the GCC and MENA regions and PMWEB Global Partner of the Year 2025, with offices in Dubai, Abu Dhabi and Riyadh. CMCS specialises in digital project management solutions for real estate developers, government entities, infrastructure owners, project management consultants and construction companies across the Middle East and North Africa.

Authority Enforced, Not Assumed — Workflows, the DoA Matrix and Delegation in PMWEB

Every approval made by the right person, within the right limit, on the record

Most project fraud passes through an approval. A wrong estimate, a favoured contractor, an inflated change order or an accelerated payment all need someone to say yes. When the owner cannot prove who said yes, under what authority and on what evidence, the approval itself becomes the fraud's best cover.

Part 1 of this series set out the governance model: a zero-tolerance policy, a procedures manual, an integrated PMIS and top management commitment. This article deals with the control that sits at the centre of all of them, approval authority. It rewrites and expands two of my earlier articles: one on whether individuals can be held to account for deceitful or unauthorised review and approval actions, and one on how well-designed output forms help prevent fraud on formally communicated transactions.

Is this article for you?

Read this if your approvals are routed as **document reviews in Aconex, a DMS or a CDE**, signed electronically on PDFs, or collected by email. The question is not whether approvals are digital, but whether the system can read the value being approved and enforce the DoA for it. If you advise clients on project governance, the adviser's checklist near the end turns this article into diagnostic questions and recommendations. Ministries of finance and sovereign funds will find a funder's lens on this topic near the end.

Where Approval Authority Breaks Down

On a capital project, the decisions most exposed to fraud are approvals: estimates, the selection of consultants, contractors and subcontractors, specified materials and their substitutes, change orders, interim payment certificates, acceptance of work in place and acceptance of material deliveries. A project team member becomes part of a deceitful act in one of two ways. Either the review or approval is made to obtain an unlawful gain, or the person takes a decision they were never authorised to take. The second is far more common, and it is the one a system can stop outright.

- **Approvals above the approver's limit.** A project director signs a change order that the DoA matrix reserves for the programme director.
- **Submitter and approver are the same person.** The segregation of duties exists in the manual but nothing enforces it.
- **Split transactions.** One change is broken into several smaller changes, each just below an approval threshold.
- **Informal delegation.** An approver on leave tells a colleague to "sign on my behalf", with no record of the scope or the period.
- **Skipped steps.** The technical review is bypassed because "the contractor needs payment this week".
- **Back-dated or undocumented decisions.** Approvals given in a meeting are recorded weeks later, if at all.

Five Ways Approval Authority Is Bypassed

'Who may approve is decided by the transaction's data, not by the sender.'

How authority is bypassed

PMWEB control



Approval above limit: Approver signs transactions exceeding their DoA matrix threshold.



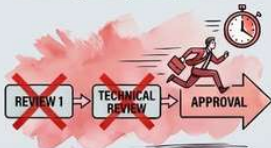
Self-approval: Submitter approves their own submitted transaction due to lack of system enforcement.



Informal delegation: Approvers verbally tell colleagues to sign on their behalf without formal records.



Split transactions: A single change is broken into smaller changes to stay below approval thresholds.



Skipped review steps: Technical or required review steps are bypassed to rush processing.



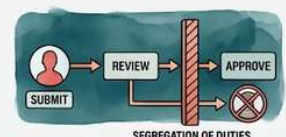
Data-driven routing: DoA branch rules automatically route transactions by value and contract impact.



Cumulative flags: Cumulative rules on commitments detect and flag split transactions.



Formal delegation: System enforces documented delegation detailing scope, period, and reason.



Segregation of duties: Workflow rules automatically exclude the submitter from all approval steps.



Enforces workflows: System enforces complete delegation detailing overdue alerts commensurate steps.



Enforced workflows: Workflows cannot complete without every step; overdue alerts escalate stalled steps.

Authority enforced, not assumed.

CMCS | PMWEB Authorised Implementation Partner – GCC & MENA

Gemini Notebook

Four Requirements for Accountable Approvals

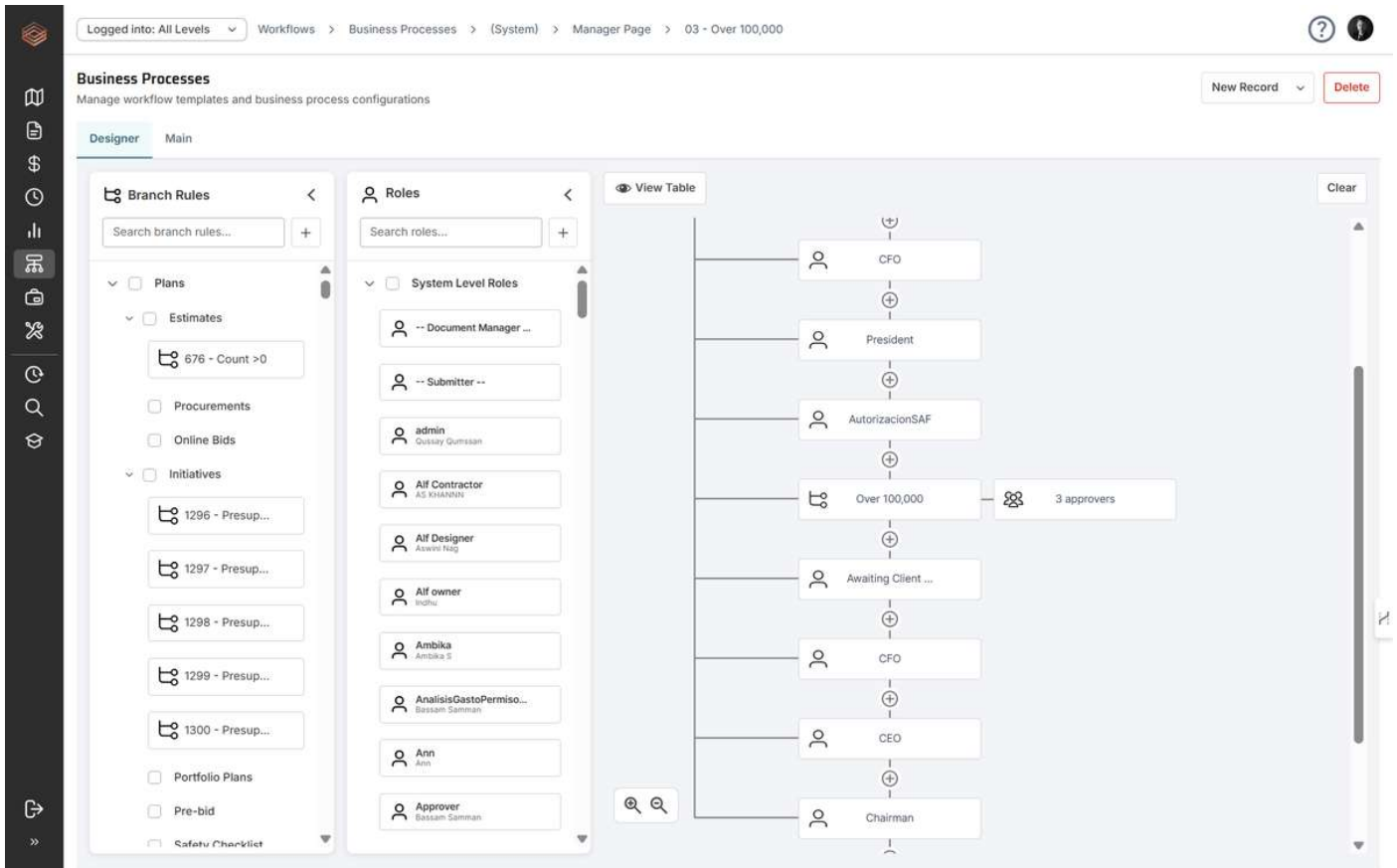
To reduce the risk of fraudulent or unauthorised review and approval, the project management plan needs four things. Each maps directly to PMWEB functionality.

Requirement	What the plan must define	How PMWEB enforces it
1. Forms	A form for every business process, with the data each role is authorised to provide	Out-of-the-box templates plus the custom form builder, with permissions on each template and each field
2. Workflows	The review and approval steps for each process and the people or roles in each step	Workflow templates with steps, roles, durations, branches and conditions
3. DoA matrix	Approval limits by role, value, category and whether the transaction changes the contract	Branch rules in each workflow that route the transaction to the authority level its attributes require
4. Delegation	A formal process for delegating or replacing approvers during absence	Workflow delegation with scope, period, reason and activation status
5. History	Automatic capture of planned and actual review and approval actions	Workflow tab and workflow log on every record, reported across the portfolio

Forms That Capture Only What Each Person Is Authorised to Provide

PMWEB comes with ready-to-use templates for the processes with the highest risk of fraudulent or unauthorised approval: requests for information, site inspections, technical and material submittals, contractor prequalification, bid comparison, contract awards, claim notices, change orders, interim payment certificates, miscellaneous invoices, budgets and budget adjustments. Processes that are not available out of the box, such as material substitution, value engineering proposals, work inspection requests and material inspection requests, are built with the custom form builder, in the language the project needs.

Permissions apply to the template as a whole and to each field within it. The contractor can enter the submitted amount on a progress invoice but cannot touch the approved amount. The cost engineer can enter the assessed value but cannot change the contract value. Each person provides exactly the information the project management plan says they are authorised to provide, and the record shows who entered each value.



Because the routing is decided by the transaction's own data, nobody can choose a friendlier approver. And because overdue alerts escalate stalled steps, nobody can sit on a transaction indefinitely to pressure a contractor.

Delegation Without Loopholes

Approvers go on leave, travel and change roles. Without a formal delegation process, their approvals are made informally by whoever is available, and the authority trail breaks. PMWEB workflow delegation records each delegation as a controlled action:

1. Select the person whose review and approval tasks are being delegated.
2. Choose whether it applies to all projects or selected projects, and to all roles the person holds or specific roles.
3. Choose a temporary delegation or a permanent replacement, and the person receiving the tasks.
4. Decide whether it covers future tasks, tasks already in progress, or both.
5. Set the end date for a temporary delegation and record the reason.
6. Activate or deactivate the delegation. Every task completed under it shows both the original approver and the delegate.

Logged into: All Levels Workflows > Role Manager > (System)

Role Manager Define Visual W

Main Opt

Search

Delega

By Use

Delegate / Replace User

User: Bassam.Z - Bassam Samman

Group by: None Layout: System Default Layout

Cancel Save

Line #	Level	Role	Action	Delegate To / Replace With*	Apply To Records	End
	(System)	-- All --	Delegate		Both	day-month-y...

No records available.

0 - 0 of 0

250 Rows

Output Forms That Tell the Whole Story

Many transactions still leave the system as a formal communication: a change order issued to the contractor, a payment certificate sent to finance, an inspection result returned to site. Whether wet-signed or digitally signed, a well-designed output form has four components. Together they make the communication self-evidencing.

Component	What it shows	Why it deters fraud
1. Transaction details	The content specific to the process: for a change order, the cause, line items, cost and time impact and the revised contract value	The figures communicated are the figures approved, drawn from the record rather than retyped
2. Verification checklist	Every item that had to be confirmed before approval, with who confirmed it and when	Shortcuts are visible; nobody can claim an item was checked when it was not
3. Supporting documents	The list of attachments and linked records sent with the transaction	The recipient knows exactly what evidence the decision rested on
4. Workflow record	Planned and actual review and approval steps: name, role, date, action, comments, delegate and, optionally, signature	Anyone receiving the form can see who approved it and under what authority

Checklists deserve emphasis. A predefined checklist, aligned with the contract's obligations and entitlements, can be added to any out-of-the-box PMWEB template; on custom forms, it is a table within the form design. Each checklist task is assigned to the person responsible and dated when completed. For a work inspection request, it lists every item to be inspected. For an RFI, it confirms the RFI is a genuine request for information and not a vehicle to create grounds for a variation.

Commitment Change Orders

Project Name

Project Number

Project Address

Telephone

Fax

Date

Boston Medical Center

RVS0104

Calle 1

Bogota, MA 02118

(617) 638-8000

30-Sep-2011 12:00:00 AM

To Subcontractor/Vendor

Contract Date

Contract Number

Change Order Number

Boston Contractors1

Commonwealth Avenue

Suite 18000

Boston, MA 010110000

30-Sep-2011 12:00:00 AM

002

001

The Contract is hereby revised by the following items:

CE #	Item #	Description	Cost Code	Amount
1 - Office Modifications		Painting		\$30,000.00
1 - Office Modifications		Carpentry		\$40,000.00
Total				\$70,000.00

The original Contract Value was.....

\$7,135,000.00

Sum of changes by prior Subcontract Change Orders.....

\$0.00

The Contract Value prior to this Subcontract Change Order was.....

\$7,135,000.00

The Contract value will be changed by this Subcontract Change Order in the amount of.....

\$70,000.00

The new Contract Value including this Subcontract Change Order will be.....

\$7,205,000.00

The Contract duration will be changed by.....

0 Days

The revised Substantial completion date as of this Subcontract change order is.....

29-Sep-2013 12:00:00 AM

Workflow

Step	All Must Approve	Due Date	Role (User)	Delegate	Instructions
No		16-Nov-2021 8:36:07 PM			
4	No	16-Nov-2021 8:36:07 PM	Superintendent (Bassam Samman)		
5	No	21-Nov-2021 8:36:07 PM	Project Accountant (Bassam Samman)		
6	No	26-Nov-2021 8:36:07 PM	Project Manager (Bassam Samman)		

1 of 2

Printed on 23-Oct-2026 10:32:42 AM

101 - PMWEB

Commitment Change Orders

Workflow Log

Step	Due Date	Role (User)	Action Date	Action Time	Action	Signature
		Bassam Samman (admin)	11-Nov-2021 8:36:07 PM	8:36 PM	Submit	<i>A. Lincoln</i>
4	16-Nov-2021 8:36:07 PM	Bassam Samman (admin)	11-May-2023 9:17:12 PM	9:17 PM	Approve	<i>A. Lincoln</i>

2 of 2

Printed on 23-Oct-2026 10:32:42 AM

101 - PMWEB

Anatomy of a Fraud-Resistant Output Form

1. Transaction Details

Figures drawn directly from approved records, never retyped manually.

2. Verification Checklist

Every required item confirmed with date and responsible party.

3. Supporting Documents

Explicit list of attachments and evidence backing the decision.

4. Workflow Record

Complete audit trail showing name, role, date, action, delegate, and signature.

Works for:

- change orders
- payment certificates
- inspections
- submittals

Anyone who receives the form can see who approved it and why.

Every output form tells the whole story.

CMCS | PMWEB Authorised Implementation Partner – GCC & MENA

Gemini Notebook

Can Individuals Be Held to Account?

My original article asked whether individuals can be accused of fraud for deceitful or unauthorised review and approval actions. Whether a specific act is fraud is a question for investigators, lawyers and courts. What a PMIS determines is whether the facts can be established. With PMWEB, every action is recorded at the time it happens: who entered each value, who reviewed, who approved, on which date, under which delegation, with which comments and

on which evidence. An approver cannot later claim they were not involved, that someone else acted without their knowledge, or that the transaction was within their authority when the DoA rule shows it was not.

That record protects honest staff as much as it exposes dishonest ones. A project manager who followed the process can show it. Without the record, everyone is equally suspect.

When the Approval Lives in the Wrong System

Many owners believe their approvals are already controlled because they are routed electronically: through document-review workflows in Aconex, another document management system or a CDE, an e-signature service, or a generic workflow tool. These approvals look digital. For fraud control they are often weaker than a wet signature, because they carry the authority of a system without the logic of one.

- **The value is invisible to the workflow.** A change order uploaded as a PDF is routed by a document-review template. The amount sits inside the file, so no rule can send a SAR 18 million change to the programme director. The DoA is applied, if at all, by the people choosing the reviewers.
- **The approved document and the paid figure can differ.** The PDF is approved in one system and the amount is keyed into the ERP in another. Nothing proves the two are the same. Every re-keying step is a fraud opportunity.
- **A signature proves identity, not authority.** An e-signature confirms who signed. It does not confirm they were authorised to approve that value, for that contract, on that date.
- **Delegation becomes account sharing.** When the approver is away, the workflow is reassigned by an administrator or the approver's login is used by a colleague. The record then shows the wrong person.
- **The audit trail records access, not decisions.** Document platforms log who viewed, downloaded or stamped a file. That is not the same as who approved what amount under which authority.

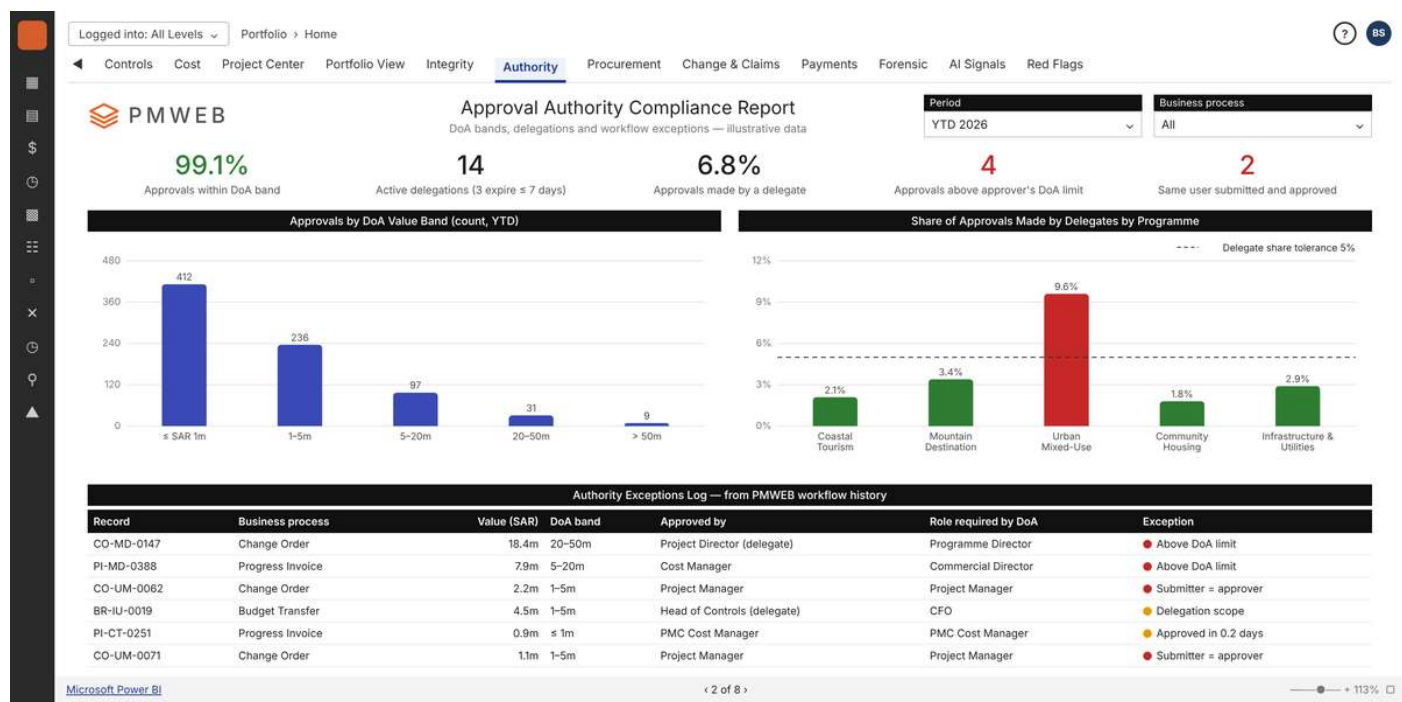
The result is false assurance: management sees a digital approval trail and assumes the DoA is enforced. In PMWEB the approval is on the transaction itself, the values are data the workflow can read, and the same approved record posts to the cost ledger and, through integration, to the ERP.

No excuse to stay on the wrong platform

If approvals in your organisation are routed as document reviews in Aconex, a DMS or a CDE, or by email, the DoA cannot be enforced on transaction value. There is no excuse for leaving it there: **migrate your approval-bearing processes to a PMIS like PMWEB**, starting with change orders and payment certificates, while keeping the document platform for correspondence through PMWEB's integrations.

Monitoring Authority Across the Portfolio

The workflow history of every record is data. Reported across all projects, it shows whether the DoA matrix is working in practice.



Approval Authority Compliance Report — Power BI on the PMWEB database, embedded in PMWEB. Illustrative data.

In the illustrative report, 99.1% of approvals fall within the correct DoA band, which looks reassuring. The exceptions log shows what the average hides: four approvals made above the approver's limit, two transactions approved by the person who submitted them, and a budget transfer approved by a delegate outside the scope of the delegation. The delegate share chart shows one programme where nearly one approval in ten is made by a delegate, twice the tolerance. Each row opens to the record and its workflow log.

Authority red flag	Rule on PMWEB data
Above DoA limit	Approved amount exceeds the limit of the approving role for that process
Submitter = approver	Same user on the submit step and any approval step of the same record
Threshold splitting	Two or more transactions on the same commitment and cause within N days, each below a DoA threshold, summing above it
Delegation outside scope	Delegate approves a process, project or role not covered by the active delegation
Implausibly fast approval	High-value approval completed in a fraction of the norm for that process and value band
Persistent overdue steps	The same approver repeatedly exceeds step duration on one contractor's transactions

Where PMWEB 2026 AI Helps

The PMWEB 2026 AI Assistant gives auditors and PMO staff a faster way into this data. A reviewer can ask it to find all change orders approved by delegates on a programme last quarter, open the record with the largest value, and create an Integrity Red Flag record linked to it, which the assistant does only once the reviewer approves the action. The assistant honours PMWEB security, so it cannot reveal records the reviewer is not permitted to see. Its help mode also explains the workflow and DoA rules configured for a process, which is useful for new staff who need to understand why a transaction was routed the way it was.

Email, Document-Platform and PMWEB Approvals Compared

Capability	Approvals by email and signature	Document platform or generic workflow	Approvals in PMWEB workflow
Routing	Chosen by the sender	Fixed by a document-review template or chosen by the sender	Decided by the transaction's value, category and contract impact

Capability	Approvals by email and signature	Document platform or generic workflow	Approvals in PMWEB workflow
Authority limits	Checked, if at all, by the approver	Not applied: the value sits inside a PDF the workflow cannot read	Enforced by branch rules from the DoA matrix
Segregation of duties	Relies on goodwill	Rarely configured; shared accounts are common	Submitter excluded from approval steps
Delegation	Verbal or by email	Administrator reassignment or account sharing	Recorded with scope, period, reason and status
Evidence of review	Scattered in inboxes	Comments on a document, not a checklist on a transaction	Checklist, comments and attachments on the record
Audit	Reconstructed after the event	Access logs showing who viewed, not who approved what value	Workflow log reported across the portfolio

The funder's lens — ministries of finance and sovereign funds

- Approvals made outside authority are the first sign that a funded entity's governance is not working. Ask for DoA compliance and off-system approvals as standard reporting lines.
- Where the funder holds reserved matters, such as large commitments or changes, those thresholds can be built into the same PMWEB workflow branches, with the funder as an approval step or notified party.

Adviser's checklist — for consultants recommending project governance

Questions to ask in the diagnostic

- Can the client's system read the value of a transaction and route it under the DoA, or does a person choose the reviewers?
- How is delegation recorded during absences, and can it be audited?
- How many approvals in the last year were above the approver's limit or made by the submitter?

Recommendations to put in the governance report

- Embed the DoA matrix as workflow rules on the transaction, not as a reference document.
- Prohibit off-system approvals for any transaction that posts to cost.
- Require output forms to carry the checklist, evidence list and workflow record.

Evidence That Authority Controls Are Working

- **DoA compliance.** Approvals outside the authorised band, trending to zero.
- **Segregation.** No record approved by its submitter.
- **Delegation discipline.** Active delegations all within scope, with an end date and a reason.
- **Off-system approvals.** No transaction posted to the cost ledger without a completed workflow.
- **Output form completeness.** Every formal communication issued with checklist, evidence list and workflow record.

Key takeaway

An approval is only a control if the system decides who may give it, records who did, and shows the evidence it rested on. PMWEB embeds the DoA matrix in workflow, formalises delegation and prints the full approval story on every output form.

An approval routed through a document platform looks controlled, but if the system cannot read the value it cannot enforce the authority.

Fraud then needs to beat the system as well as the people, and anyone who tries leaves a record.

Moving approval-bearing processes to PMWEB is what turns the DoA from a document into a control.

Next in the series: Part 3 moves to procurement: how PMWEB prequalification, bid comparison against the approved estimate and line-item analysis expose unqualified bidders, unbalanced bids and front-loading before the contract is signed.

Talk to us: If your projects run on Aconex or another document management system, a CDE without DoA-driven workflows, a PMIS without ERP integration or full cost and contract management, or no system at all, there is no longer an excuse to stay: migrate your fraud-exposed processes to a PMIS like PMWEB. CMCS can assess your current platforms and data, start PMWEB on a new programme, integrate it with your ERP and document platforms, and migrate legacy project data, including from Oracle Aconex and Oracle Unifier. Contact CMCS at info@CMCS-MENA.com. Management consultants designing project governance for their clients are welcome to use these frameworks; CMCS works alongside consulting firms to turn governance recommendations into configured PMWEB processes. Ministries of finance and sovereign funds can also see how a common PMWEB standard across funded entities gives them verified, portfolio-wide visibility.

#PMWEB #CMCS #FraudPrevention #DelegationOfAuthority #Workflow #PMO #CapitalProjects #ProjectControls #PMIS #Governance #CDE #DocumentManagement #ERPIntegration #ManagementConsulting #ProjectGovernance #MinistryOfFinance #SovereignWealthFund

About the Author

Bassam Samman, PMP, PSP, EVP, GPM is the Chairman and Chief Executive Officer of CMCS FZCO, the PMWEB Authorised Implementation Partner for the Gulf Cooperation Council and broader Middle East and North Africa region. CMCS holds the PMWEB Global Partner of the Year 2025 designation and serves capital project owners, contractors and consultants across the UAE, Saudi Arabia, Qatar and Kuwait.

Bassam has over four decades of experience providing project management, project controls services and project management information systems to more than two hundred capital projects with a combined value exceeding one hundred billion US dollars. He is the author of four published books on project management digitalisation, and has lectured at more than three hundred and fifty international events. He is a co-founder of the Project Management Institute Arabian Gulf Chapter. He holds a Master's degree in Engineering Administration (Construction Management), with Faculty Commendation, from George Washington University and a Bachelor's degree in Civil Engineering from Kuwait University, with executive education at Harvard Business School and London Business School.

About PMWEB

PMWEB is an enterprise-class, web-based capital construction project management platform trusted by organisations worldwide including Harvard University, the United Nations, and Atlanta Airport. Built on Microsoft .NET technology, PMWEB manages the entire project lifecycle within a single integrated platform — from portfolio planning and cost management through document control, procurement, scheduling, asset management, and business intelligence. With 150+ pre-configured SSRS reports, drag-and-drop dashboard design, multi-currency support, and open REST/SOAP API integration, PMWEB delivers enterprise capability with implementation timelines measured in months, not years.

About CMCS

CMCS (Collaboration, Management and Control Solutions) is the PMWEB Authorised Implementation Partner for the GCC and MENA regions and PMWEB Global Partner of the Year 2025, with offices in Dubai, Abu Dhabi and Riyadh.

CMCS specialises in digital project management solutions for real estate developers, government entities, infrastructure owners, project management consultants and construction companies across the Middle East and North Africa.

Procurement Integrity — Prequalification, Bid Analysis and Unbalanced Bids in PMWEB

Stopping fraud before the contract is signed

The most expensive fraud on a capital project is often decided before the first shovel enters the ground. An unqualified bidder invited, an unbalanced bid accepted, a design error known to one bidder and not the others: each turns the contract itself into the vehicle for loss.

Part 2 showed how PMWEB enforces approval authority on every transaction. This article applies those controls to the procurement cycle, where the value at stake is largest and the window to act is shortest. Once a contract is signed, a flawed award is very hard to unwind. The owner pays for it in change orders, claims and acceleration costs for the rest of the project.

Is this article for you?

Read this if bids arrive as attachments in an e-tendering portal, a **document platform such as Aconex** or by email, or if your **PMIS has no estimate, bid comparison and commitment chain** connecting the evaluated rates to the contract and its changes. If you advise clients on project governance, the adviser's checklist near the end turns this article into diagnostic questions and recommendations. Ministries of finance and sovereign funds will find a funder's lens on this topic near the end.

A Case That Shows How It Works

Case: the pile design that everyone but the owner knew about

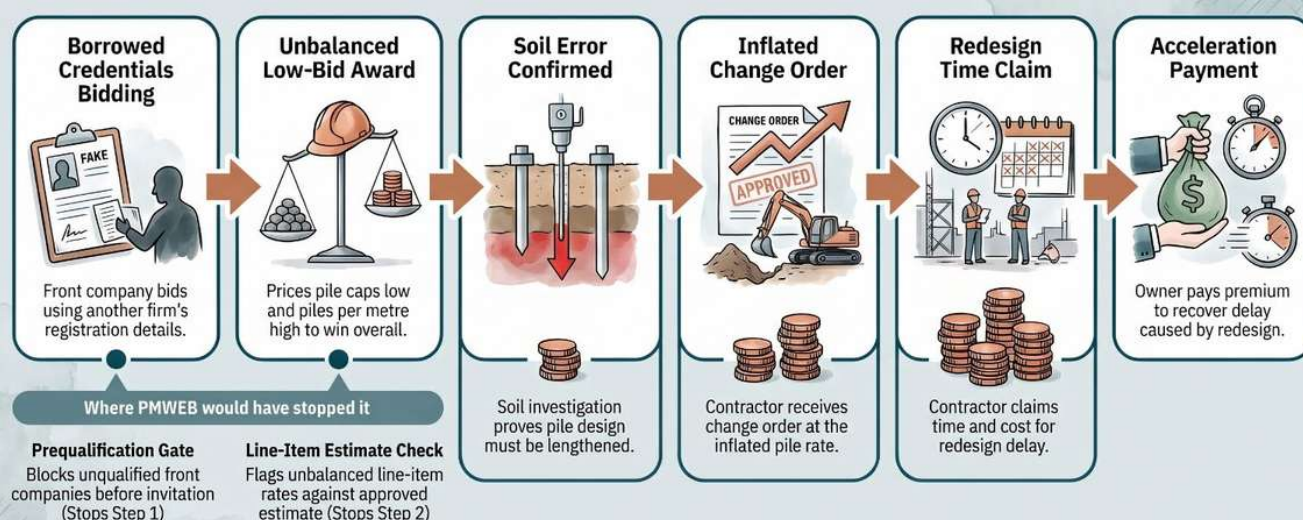
On a major building project, a contracting company was formed specifically to bid. It used another firm's registration credentials to be accepted onto the tender list. Its founders had inside information that the pile design in the tender documents was wrong: after a post-award soil investigation, the piles would have to be redesigned and lengthened.

The new company unbalanced its bid accordingly. It priced pile caps, which would not change, very low, and priced piles by the metre, which would grow, well above market. Its total was the lowest, and it won.

After award, the soil investigation confirmed the error. The piles were redesigned and extended. The contractor received a change order at its inflated pile rate, then claimed time and cost for the redesign, and was finally paid for a directive acceleration to recover the delay.

At least three failures by the owner's team made this possible: an incorrect soil investigation and design, an unqualified contractor invited to bid, and an unbalanced bid accepted without challenge. The last two are procurement controls that a PMIS enforces.

Anatomy of an Unbalanced Bid



The cheapest place to stop procurement fraud is before award.

When a bid looks too good, ask why – before you sign.

CMCS | PMWEB Authorised Implementation Partner – GCC 0. MCMA Gemini Notebook

Six Questions Every Bid Analysis Must Answer

My earlier article on machine learning for fraud detection used the bid analysis report as its example, because a single report can expose six possible fraud transactions. Each question needs specific data, captured in a structured form, to be answered with evidence rather than opinion.

Question	Fraud it exposes	PMWEB data that answers it
1. Was every invited bidder qualified at the date of invitation?	Unqualified or front companies on the bid list	Vendor prequalification records, scores and approval dates
2. Did enough compliant bids arrive to meet the minimum?	Restricted competition; cover bidding	Bid package invitees and received bids
3. Is any bid unbalanced or front-loaded?	Pricing designed to exploit expected changes or early cash	Bid line items against estimate line items
4. Is the approved cost estimate consistent with the bids received?	Estimate manipulated to justify the award or the budget	Cost estimate revisions and bid totals
5. Was the technical evaluation completed?	Award on price alone to a bidder who cannot deliver	Technical scoring on the bid package
6. Was the recommendation reviewed and approved per the DoA?	Award by someone without authority, or without review	Workflow history on the bid analysis record

Prequalification as a Gate, Not a Formality

The PMWEB vendor prequalification module holds each company's registration details, departments, contacts, insurances, applications and scoring. The scoring questionnaire is configured by the owner: years in business, comparable projects completed, financial capacity, key staff, health and safety record, pending claims and disputes, and conflict-of-interest declarations. Each question carries points and a weight; the weighted score decides whether the company is qualified for a category and value band.

The prequalification decision itself has a workflow. Procurement reviews documents, finance reviews financial statements, the technical team reviews experience, and the approver is set by the DoA. Each reviewer's comments and dates are recorded. In the case above, a company with no history, no financial record of its own and borrowed credentials would have failed at this gate, and the reviewers who passed it would be on record.

Logged into: All Levels > Tools > Vendor Prequal Records > Manager Page > 719354.2014 - Finkrock

719354.2014 Approved

Vendor Prequal Records: 719354.2014 -

Main Addresses Departments Contacts Insurance Applications **Scoring 12.5** Ratings Notes Attachments 1 Notifications Specifications

Group by: None Layout: System Default Layout New Line Add Scoring

☐	Line	Group	Question ID	Question	Answer	Score	Points Available	Weight	Weighted Score	Use	Notes
☐	1	GREEN	91	policy and methodology in m...		0	100	20 %	0	Yes	
☐	2	GREEN	92	recycle waste building mater...		0	100	20 %	0	Yes	
☐	3	GREEN	93	using recycled material for t...		0	100	20 %	0	Yes	
☐	4	GREEN	94	use of low-emission constru...		0	100	20 %	0	Yes	
☐	5	GREEN	95	using solar power for site off...		0	100	20 %	0	Yes	
☐	6	Experience	1	Relevance of Completed Work		0	10	0 %	0	Yes	The technical value of
☐	7	Experience	2	Details of Similar Projects		0	10	0 %	0	Yes	The contractor's histor
☐	8	Experience	3	Value of Completed Work	\$0.00	0	8	0 %	0	Yes	The financial value of
☐	9	Organization	4	Résumés of Key Personnel		0	5	0 %	0	Yes	The contractor's key p
☐	10	Organization	5	Organizational Structure		0	5	0 %	0	Yes	The contractor's organ
☐	11	Organization	6	Organization Resources		0	10	0 %	0	Yes	The amount of resourc
☐	12	Organization	7	Organization Methodology		0	8	0 %	0	Yes	The methodology is a
☐	13	Organization	8	Quality Control Program		0	8	0 %	0	Yes	The contractor quality
☐	14	Organization	9	Safety Policy Statement, Rec...		0	8	0 %	0	Yes	A contractor's safety n
☐	15	Organization	10	Organization References		0	10	0 %	0	Yes	References can be ver
☐	16	Organization	11	Membership Affiliations and ...		0	5	0 %	0	Yes	Contractor's members
☐	17	Organization	12	Organization Litigations		0	8	0 %	0	Yes	The past and current h

Bid packages in PMWEB draw their invitees from the prequalified vendor list. A rule can flag any invitation to a company whose qualification had not been approved by the invitation date, or had expired, which is how the dashboard later in this article counts bidders who were invited before they were qualified.

Bid Comparison Against the Approved Estimate

The approved cost estimate is the owner's independent view of what the work should cost. In PMWEB it is held line by line, with quantities, units and rates, and every revision is kept. The procurement module then holds each bidder's prices against the same bid items, alongside the estimated unit cost and total. With that structure, the comparison is calculated rather than eyeballed:

- **Bid-to-estimate ratio per line item.** Bid rate ÷ estimate rate for every item and every bidder.
- **Unbalancing.** Items priced far below estimate in one bid while others in the same bid sit far above, especially where the high items are quantity-driven or likely to change.
- **Front-loading.** Early activities such as mobilisation, preliminaries and substructure priced high, and later activities low, to accelerate cash flow and reduce the contractor's exposure if it defaults.
- **Outlier totals.** A lowest bid well below the estimate and below the other bids, which warrants a scope and assumption review rather than a celebration.
- **Identical patterns.** Bids from different companies with near-identical rates or errors, which may indicate collusion.

Logged into: All Levels Plans > Bid Packages > Manager Page > 1 - Demo Package Completed

RVS0104 - Boston Medical Center Approved

Bid Packages: 1 - Demo Package Completed

Main **Bid Items** BID RFIs Specifications Scoring Manage Bids Notes Attachments 3 Clauses Notifications

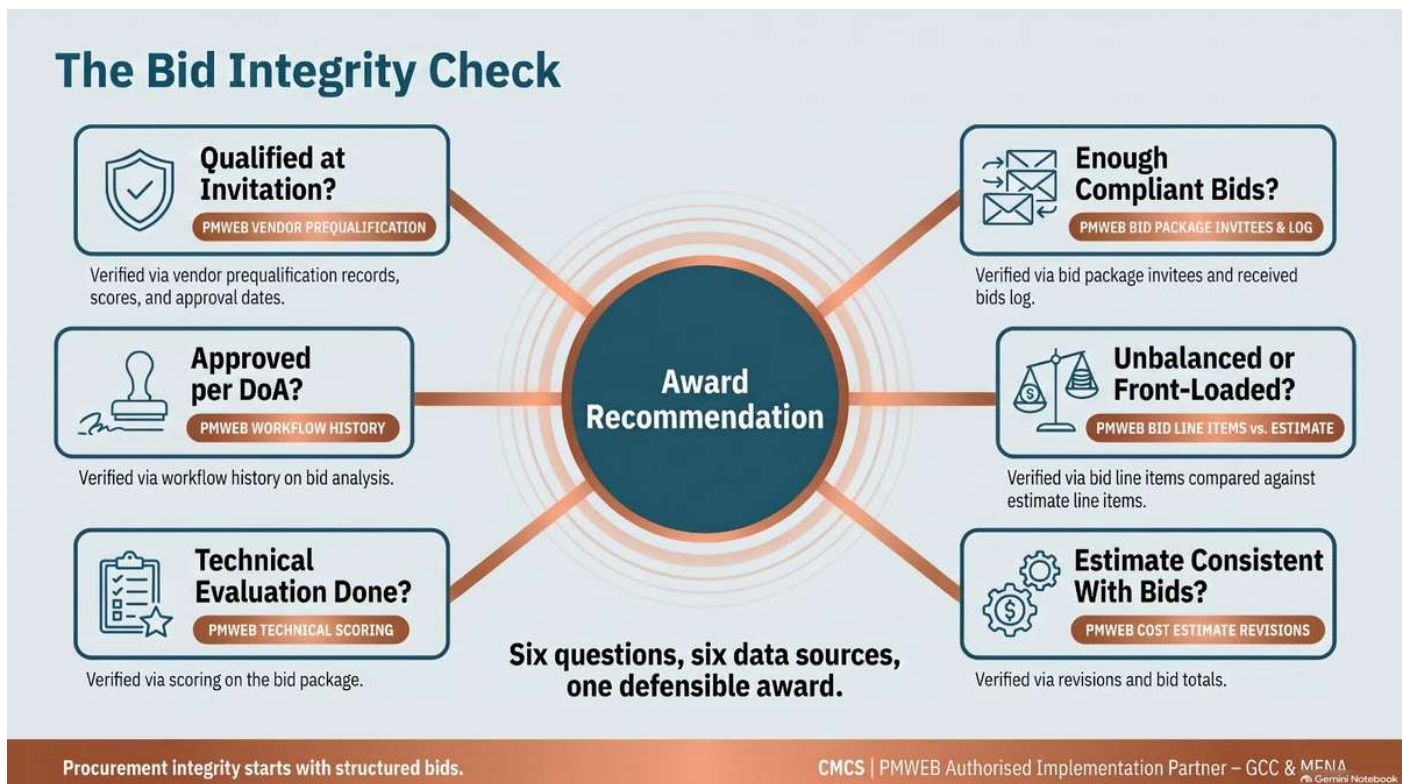
Group by: None Layout: System Default Layout

New Line Add Estimate Items Add Items Preview Conversions

Include In Bid	Line #	Attachments	Project*	Item	Description	Scope Of Work	Currency	UOM	Cost Code	Account	Asset Life and
☒	1	(0)	RVS0104 - Boston ...	2680	010000 - General R...		USD - Dollar ...				
☒	2	(0)	RVS0104 - Boston ...	2834	020000 - Existing ...		USD - Dollar ...				
☒	3	(0)	RVS0104 - Boston ...	2889	030000 - Concrete		USD - Dollar ...				
☒	4	(0)	RVS0104 - Boston ...	2998	040000 - Masonry		USD - Dollar ...				
☒	5	(0)	RVS0104 - Boston ...	3066	050000 - Metals		USD - Dollar ...				
☒	6	(0)	RVS0104 - Boston ...	3158	060000 - Wood, Pl...		USD - Dollar ...				
☒	7	(0)	RVS0104 - Boston ...	3300	070000 - Thermal a...		USD - Dollar ...				
☒	8	(0)	RVS0104 - Boston ...	3512	080000 - Openings		USD - Dollar ...				
☒	9	(0)	RVS0104 - Boston ...	3741	090000 - Finishes		USD - Dollar ...				
☒	10	(0)	RVS0104 - Boston ...	4267	120000 - Furnishings		USD - Dollar ...				
☒	11	(0)	RVS0104 - Boston ...	4522	140000 - Conveyin...		USD - Dollar ...				
☒	12	(0)	RVS0104 - Boston ...	4588	210000 - Fire Suppr...		USD - Dollar ...				
☒	13	(0)	RVS0104 - Boston ...	4633	220000 - Plumbing		USD - Dollar ...				
☒	14	(0)	RVS0104 - Boston ...	4763	230000 - Heating, ...		USD - Dollar ...				

1 - 39 of 39

Unbalanced items are not proof of fraud. Contractors price risk differently, and a low rate may reflect a genuine efficiency. They are, however, a signal to go back to the tender documents and ask a specific question: is there something about this item's quantity or design that this bidder knows and the owner does not? In the case above, that question asked of the pile items would have exposed the design error before award.



Online Tendering Is Not Procurement Control

Owners often point to their e-tendering portal or ERP sourcing module as proof that procurement is digital and transparent. Those tools are valuable: they control access to tender documents, time-stamp submissions and keep bids sealed until opening. But they were designed to manage the tender event, not the integrity of the award. Used as the only procurement system, they create false assurance in three ways.

- **Bids arrive as attachments.** The priced bill of quantities is an uploaded spreadsheet or PDF. The portal compares totals; nobody compares every line item with the approved estimate, so unbalanced rates such as the piling case pass unseen.
- **Prequalification is a document upload.** Certificates and financial statements are attached but not scored, weighted or approved through a DoA workflow. A front company with borrowed credentials can upload the same files as a genuine contractor.
- **The evaluated rates disappear at award.** The ERP purchase order is created with a total or retyped rates. When change orders arrive months later, nobody can check them against the rates that were evaluated, because those rates live in a closed tender event.

"Procurement is online" is then reported as "procurement is controlled". PMWEB closes the gap by holding prequalification scores, the estimate, every bidder's line items and the recommendation as related records, and by turning the winning bid into the commitment's schedule of values.

A PMIS can create the same false assurance if it lacks comprehensive cost and contract management. If the estimate lives in one tool, bids in a portal, contracts in the ERP and changes in correspondence, there is no single chain from evaluated rate to paid rate, and the unbalanced bid in the case above would be just as invisible as it was on paper.

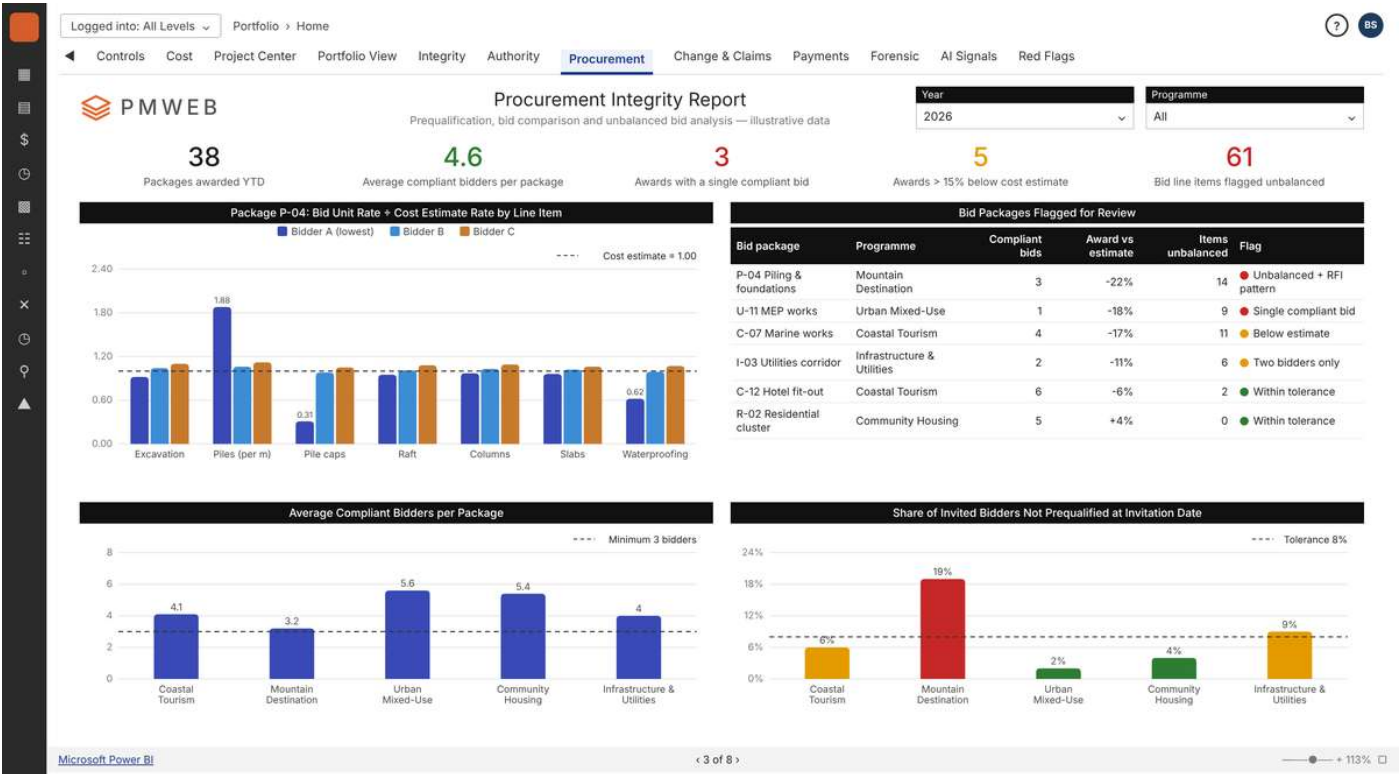
From Award to Contract Without Re-keying

Once the recommendation is approved, the successful bid's line items become the commitment's schedule of values in PMWEB. Nothing is retyped, so the rates paid on future change orders and progress invoices are exactly the rates evaluated at award. If a change order later uses a rate that differs from the contract rate for the same item, PMWEB data shows it immediately.

No excuse to stay on the wrong platform

If bids arrive as attachments and the evaluated rates never reach the contract, procurement fraud will stay invisible however carefully the tender is run. **Moving prequalification, bid comparison and commitments to a PMIS like PMWEB** is the single most effective procurement control an owner can add.

Procurement Integrity Across the Portfolio



Procurement Integrity Report — Power BI on the PMWEB database, embedded in PMWEB. Illustrative data.

The top-left chart reproduces the pattern from the case. For package P-04, Bidder A, the lowest, is priced at nearly twice the estimate rate for piles per metre and less than a third of it for pile caps, while Bidders B and C track the estimate closely. The flagged packages table shows that P-04 also carries a later RFI pattern on piling, which Part 4 will follow. The bottom charts show competition and qualification by programme: one programme averages barely three compliant bidders per package and has invited almost one in five bidders before their qualification was approved.

Procurement red flag	Rule on PMWEB data
Bidder not prequalified at invitation	Invitation date earlier than prequalification approval date, or qualification expired
Single or too few compliant bids	Compliant bids below the minimum set in the procurement policy
Unbalanced line items	Item ratio below 0.5 or above 1.5 of estimate on items carrying a set share of value
Front-loading	Share of contract value in the first 25% of the schedule well above the estimate's share
Award far below estimate	Awarded total more than a set percentage below the approved estimate
Estimate revised to fit the bids	Estimate revision approved after bid opening and before award
Repeat winner with the same evaluator	Same company and same evaluation panel member across several awards

Where PMWEB 2026 AI Helps

Bid evaluation is detailed work under deadline pressure. The PMWEB 2026 AI Assistant shortens the search part of it: a procurement auditor can ask it to find all bid packages on a programme awarded below estimate this year, open the package with the largest gap, and open the prequalification record of the winning bidder, without navigating menus. When a red flag is warranted, the assistant can create the record with the auditor's approval. Comparing line-item patterns across hundreds of packages and years, the kind of analysis that reveals a bidder who always prices the same items low, is where analytics on PMWEB data come in, and Part 7 covers that.

Spreadsheets, E-Tendering Portals and PMWEB Compared

Capability	Spreadsheet evaluation	E-tendering portal or ERP sourcing	PMWEB procurement
Bidder qualification	Checked against a list someone maintains	Certificates uploaded, not scored or approved per DoA	Drawn from approved prequalification records with dates
Estimate comparison	Estimate pasted in, version uncertain	Totals compared; estimate rarely held at line level	Approved estimate revision linked to the package
Line-item analysis	Manual, often skipped under time pressure	BOQs received as attachments; line analysis manual	Ratios calculated for every item and bidder
Evaluation record	Final spreadsheet, history lost	Submission log of the tender event	Scores, comments and approvals on the record
Award to contract	Rates retyped into the contract	Purchase order created with totals or retyped rates	Bid items become the commitment schedule of values
Portfolio view	None	Limited to the portal's own tender events	Patterns across packages, programmes and years

The funder's lens — ministries of finance and sovereign funds

- Procurement is where value for money is won or lost for the life of the contract. Ask funded entities to report award-versus-estimate, compliant bids per package and unbalanced items flagged before award.
- A single procurement standard across all funded entities lets the ministry or fund compare contractors, rates and outcomes across the whole portfolio.

Adviser's checklist — for consultants recommending project governance

Questions to ask in the diagnostic

- Are bidders' qualifications scored and approved before invitation, with dates?
- Is every bid compared line by line with the approved estimate, and is that comparison retained?
- Do the evaluated rates flow into the contract without re-keying?

Recommendations to put in the governance report

- Make prequalification a system gate tied to the procurement DoA.
- Require documented clarification of every unbalanced line item before award.
- Carry the winning bid's line items into the commitment so later changes can be tested against them.

Evidence That Procurement Controls Are Working

- **Qualified invitations.** Every invited bidder qualified for the category and value band at the invitation date.
- **Competition.** Compliant bids per package at or above policy minimum, by programme.
- **Unbalancing challenged.** Every flagged line item has a documented clarification before award.
- **Estimate stability.** No estimate revisions approved between bid opening and award without a recorded reason.
- **Post-award change on flagged items.** Change value on items flagged at award, tracked to see whether the flag was right.

Key takeaway

Procurement fraud is cheapest to stop before award and most expensive to recover after it. PMWEB makes prequalification a gate, compares every bid line against the approved estimate, and carries the evaluated rates straight into the contract.

An e-tendering portal makes the tender event secure; only a PMIS makes the award defensible.

When a bid looks too good, the data tells the owner which question to ask while there is still time to ask it.

Moving procurement into PMWEB is the most effective procurement control an owner can add.

Next in the series: Part 4 follows the contract after award: how linking RFIs, potential change orders, change orders and claims in PMWEB exposes design errors being paid for, over-priced changes and claim-oriented contractors.

Talk to us: If your projects run on Aconex or another document management system, a CDE without DoA-driven workflows, a PMIS without ERP integration or full cost and contract management, or no system at all, there is no longer an excuse to stay: migrate your fraud-exposed processes to a PMIS like PMWEB. CMCS can assess your current platforms and data, start PMWEB on a new programme, integrate it with your ERP and document platforms, and migrate legacy project data, including from Oracle Aconex and Oracle Unifier. Contact CMCS at info@CMCS-MENA.com. Management consultants designing project governance for their clients are welcome to use these frameworks; CMCS works alongside consulting firms to turn governance recommendations into configured PMWEB processes. Ministries of finance and sovereign funds can also see how a common PMWEB standard across funded entities gives them verified, portfolio-wide visibility.

#PMWEB #CMCS #FraudPrevention #Procurement #UnbalancedBids #Prequalification #CapitalProjects #ProjectControls #PMIS #CostManagement #CDE #DocumentManagement #ERPIntegration #ManagementConsulting #ProjectGovernance #MinistryOfFinance #SovereignWealthFund

About the Author

Bassam Samman, PMP, PSP, EVP, GPM is the Chairman and Chief Executive Officer of CMCS FZCO, the PMWEB Authorised Implementation Partner for the Gulf Cooperation Council and broader Middle East and North Africa region. CMCS holds the PMWEB Global Partner of the Year 2025 designation and serves capital project owners, contractors and consultants across the UAE, Saudi Arabia, Qatar and Kuwait.

Bassam has over four decades of experience providing project management, project controls services and project management information systems to more than two hundred capital projects with a combined value exceeding one hundred billion US dollars. He is the author of four published books on project management digitalisation, and has lectured at more than three hundred and fifty international events. He is a co-founder of the Project Management Institute Arabian Gulf Chapter. He holds a Master's degree in Engineering Administration (Construction Management), with Faculty Commendation, from George Washington University and a Bachelor's degree in Civil Engineering from Kuwait University, with executive education at Harvard Business School and London Business School.

About PMWEB

PMWEB is an enterprise-class, web-based capital construction project management platform trusted by organisations worldwide including Harvard University, the United Nations, and Atlanta Airport. Built on Microsoft .NET technology, PMWEB manages the entire project lifecycle within a single integrated platform — from portfolio planning and cost management through document control, procurement, scheduling, asset management, and business intelligence. With 150+ pre-configured SSRS reports, drag-and-drop dashboard design, multi-currency support, and open REST/SOAP API integration, PMWEB delivers enterprise capability with implementation timelines measured in months, not years.

About CMCS

CMCS (Collaboration, Management and Control Solutions) is the PMWEB Authorised Implementation Partner for the GCC and MENA regions and PMWEB Global Partner of the Year 2025, with offices in Dubai, Abu Dhabi and Riyadh. CMCS specialises in digital project management solutions for real estate developers, government entities,

infrastructure owners, project management consultants and construction companies across the Middle East and North Africa.

Change Without Cover — Tracing RFIs, PCOs, Change Orders and Claims in PMWEB

When design errors, over-priced changes and claim strategies leave a data trail

Change is where an unbalanced bid pays out, where a design error is quietly passed to the owner, and where a claim-oriented contractor earns its margin. Every one of those outcomes depends on a chain of documents. When the chain is linked in one system, the pattern becomes visible.

Part 3 ended with a contractor that won a piling package with an unbalanced bid, knowing the pile design would change. This article follows what happens next. It draws on my earlier articles on contract administration and on training machines to detect fraud, both of which argued that RFIs, potential change orders, change orders and claims must be linked, not managed as separate logs.

Is this article for you?

Read this if RFIs, variations and claims on your projects travel as **correspondence in Aconex, a DMS or a CDE**, or if your **PMIS manages RFIs but not the PCO, change order and commitment records** their answers lead to. If you advise clients on project governance, the adviser's checklist near the end turns this article into diagnostic questions and recommendations. Ministries of finance and sovereign funds will find a funder's lens on this topic near the end.

How Change Becomes a Fraud Channel

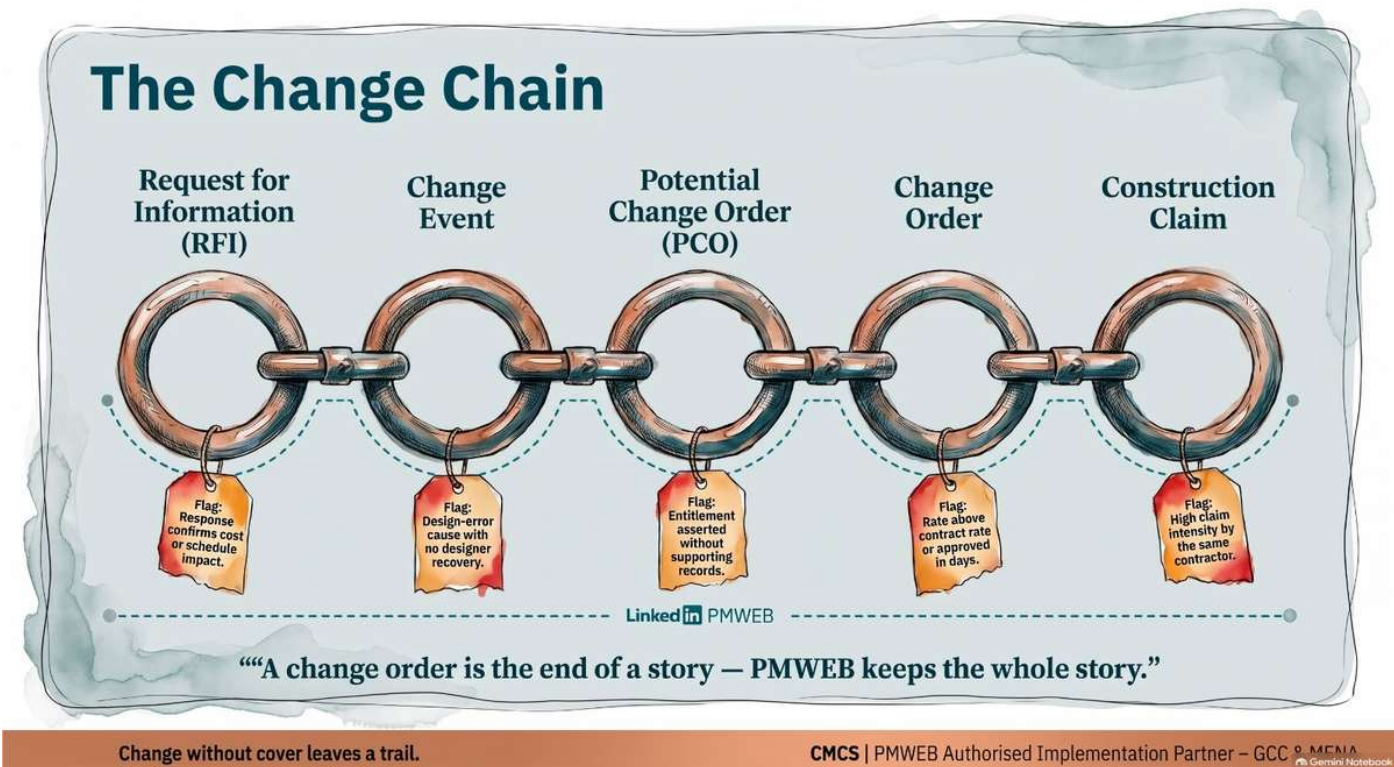
- **Unsubstantiated change orders.** Approved without a clear cause, entitlement or supporting records.
- **Over-estimated change orders.** Priced at rates or quantities above the contract or market, often on items the contractor priced high at bid.
- **Design errors paid twice.** The designer's error becomes a contractor change paid by the owner, while the designer's liability is never pursued.
- **RFIs used to manufacture variations.** Questions raised not to clarify but to create grounds for a change or a claim.
- **Claims by strategy.** A contractor bids low and recovers margin through a high volume of RFIs, notices and claims, project after project.
- **Acceleration paid for self-inflicted delay.** The owner pays to recover time that the contractor's own performance lost.

The Change Chain in PMWEB

PMWEB manages change as a connected chain of records, each with its own template, attachments and workflow. The links between them are what make the chain auditable.

Record	Purpose	Link that matters
RFI	The contractor's question on an ambiguity, discrepancy or error in the documents, and the designer's response	Linked to the PCO or change order it gives rise to; tagged when the response identifies cost or time impact
Change event	The event that may affect cost or time, raised by any party	Groups the PCOs and change orders it causes across commitments
Potential change order (PCO)	The contractor's notice of an event it believes entitles it to a change, with supporting records	Linked to the RFI, the change event and, if approved, the change order

Record	Purpose	Link that matters
Change order	The approved adjustment to contract value and time, owner-directed or from an approved PCO	Line items tied to the commitment's schedule of values and cost codes
Claim	The contractor's formal claim for time and money under a contract clause	Linked to notices, PCOs, affected schedule activities and the counterclaim response



RFIs that carry cost

Design errors and omissions are usually discovered by the contractor, who raises an RFI. The designer's response may recommend additional work, which leads to a change order. PMWEB has a built-in link between RFIs and change orders, so every change caused by an RFI response can be traced back to the question, the designer's answer and the date of each. In the piling case, the contractor's RFI reporting the soil investigation and its effect on the pile design should have raised one alert, and the designer's response confirming cost and time impact should have raised a second. Both would also point to the designer's liability.

A checklist on the RFI template helps separate genuine questions from engineered ones: the RFI is a request for information already in the contract documents, it does not instruct a change, it is the only RFI on the subject, and it is not raised to create grounds for a variation. Each item is confirmed by the reviewing engineer.

Logged into: All Levels > Schedules > Claim Analysis Worksheet > Manager Page > Claim Analysis Worksheet (New)

Claim Analysis Worksheet (New) Draft

Cancel Save

Main

PMWeb
Plan | Build | Operate™

Claim Analysis Worksheet

Project: [Dropdown] ID: 1 Date: 23-Oct-2026 12:3... [Calendar]

Contractor: [Dropdown]

Claim Title: [Text Field]

Revision: 0 Status: Draft Date: 23-Oct-2026 12:36:19 tt [Calendar]

Claim Analysis Worksheet

Claim Analysis Worksheet

Category	Item	Submi...	Remarks
No records available.			

0 - 0 of 0 250 Rows

Details of Remarks

Correspondence Platforms Hold the Letters, Not the Change

On many projects, RFIs, change requests, variation orders and claim notices are exchanged through a correspondence platform such as Aconex, a document management system or a CDE, as letters and transmittals. The owner can show that every document is filed, numbered and searchable, and concludes that change is under control. For fraud control, that conclusion is false.

- **The cost impact is trapped in the attachment.** An RFI response that admits a design error, or a variation priced at an inflated rate, is a PDF. No rule can read its amount, its cause or the contract items it affects.
- **Links are between documents, not data.** A letter can reference an earlier letter. It cannot link a change order's line items to the commitment's schedule of values, so rates above contract rates go unnoticed.
- **Design liability disappears.** Because the cause of each change is not captured as a value, the owner cannot total how much it has paid for design errors, or pursue the designer for it.
- **Claim strategies look like normal correspondence.** A contractor raising three times the portfolio rate of RFIs and claim notices simply generates more mail. Without structured data across projects, the pattern is invisible.

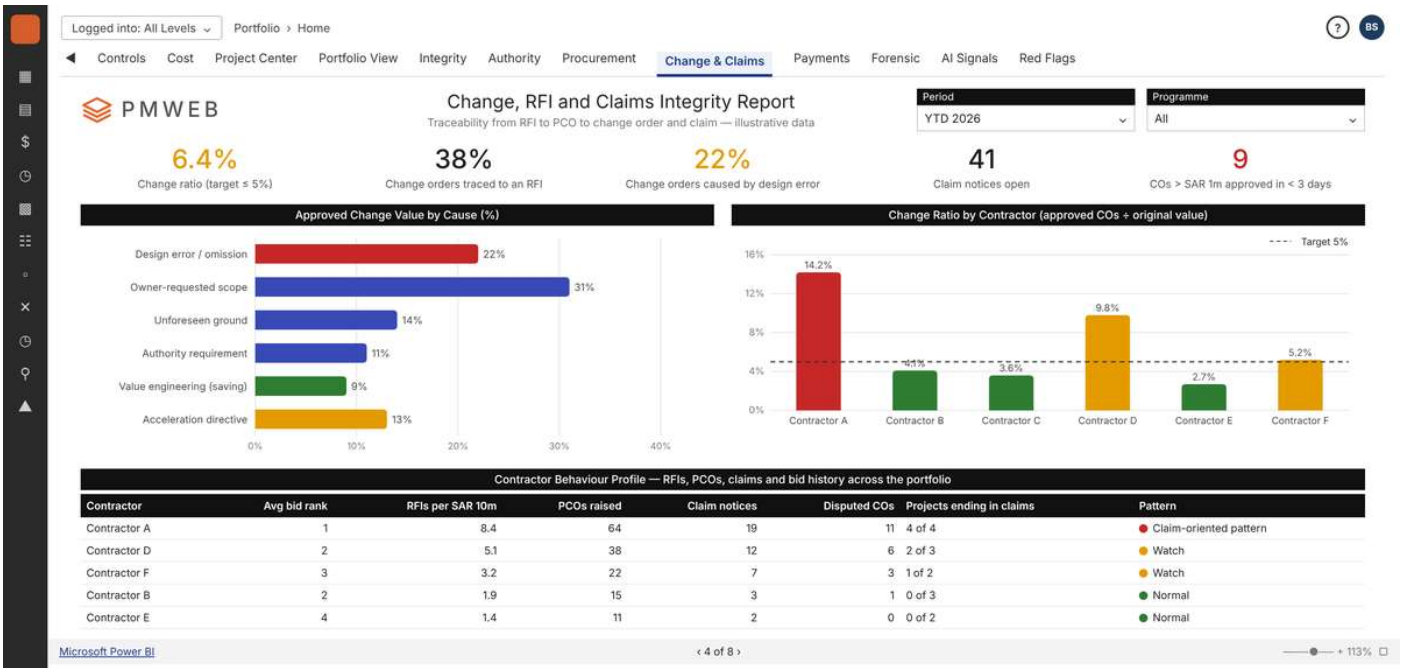
Correspondence control is necessary, and PMWEB integrates with Aconex, Autodesk ACC, SharePoint and Egnyte where an owner keeps one. But the change itself, its cause, value, time impact, entitlement and approval, has to be managed as a structured chain of records, or the owner is filing the evidence of fraud without ever detecting it.

No excuse to stay on the wrong platform

If change lives as correspondence in Aconex, a DMS or a CDE, or your PMIS stops at the RFI, the cost of design errors, over-priced changes and claim strategies cannot be measured. **Migrating the change chain to a PMIS like PMWEB**, integrated with your document platform during transition, turns that correspondence into controllable data.

Spotting the Claim-Oriented Contractor

One project rarely reveals a strategy. The portfolio does. When RFIs, PCOs, claims and bid history for every contract sit in one database, a pattern can emerge: a contractor that always bids lowest, raises far more RFIs per unit of contract value than its peers, issues a stream of claim notices, and ends most of its projects in claims or disputes. Its prequalification submission may even show pending claims with other owners. None of this proves wrongdoing, but it tells the owner how to price risk, what to watch and whether the next invitation is wise.



Change, RFI and Claims Integrity Report — Power BI on the PMWEB database, embedded in PMWEB. Illustrative data.

In the illustrative report, more than a fifth of approved change value is attributed to design errors and omissions, a figure the owner should be recovering from designers rather than absorbing. Contractor A has a change ratio nearly three times the target, the lowest average bid rank, the highest RFI rate and four of four projects ending in claims. Nine change orders above SAR 1 million were approved in under three days, quicker than any genuine review of entitlement and pricing allows.

Change and claims red flag	Rule on PMWEB data
Change on items unbalanced at award	Change order line items on bid items flagged at award, especially quantity increases
Rate above contract rate	Change order unit rate differs from the commitment schedule of values rate for the same item
Design-error changes without designer recovery	Change orders with cause = design error and no linked back-charge or notice to the designer
RFI-to-CO in days	Change order approved within a few days of the linked RFI response, above a value threshold
High RFI and claim intensity	RFIs and claim notices per SAR 10 million of contract value well above the portfolio norm
Acceleration after contractor delay	Acceleration change order where the schedule shows contractor-caused critical delay
Change ratio drift	Approved changes ÷ original contract value rising above tolerance, by contract and by contractor

Where PMWEB 2026 AI Helps

Change and claims files are long and document-heavy. The PMWEB 2026 AI Assistant helps reviewers move through them quickly: find every RFI on a contract whose response flagged cost impact, open the linked change orders, and find all claim notices citing a given clause across the programme. When a reviewer wants to record a concern, the assistant creates the red flag or a notice to the designer with the reviewer's approval. The deeper analysis, for example

comparing each contractor's RFI and claim intensity against hundreds of past contracts, belongs to analytics on PMWEB data, which Part 7 explains.

Separate Logs, Correspondence Platforms and a Linked Change Chain

Capability	Separate logs and correspondence	Document platform or CDE	Linked change chain in PMWEB
RFI to change	Connection in someone's memory	Letters cross-referenced; no cost or cause data	Built-in link from RFI to change order
Entitlement	Asserted in letters	Argued in attached documents	PCO with supporting records before any change order
Pricing	Rates negotiated case by case	Priced in PDFs, not against the schedule of values	Line items against contract schedule of values
Design liability	Rarely pursued	Cause not captured, so never totalled	Design-error cause tracked and linked to back-charges
Claims file	Assembled when the dispute starts	Correspondence found by search when the dispute starts	Built record by record from the first notice
Contractor behaviour	Anecdote	More mail, but no pattern across projects	RFI, PCO, claim and bid history across the portfolio

The funder's lens — ministries of finance and sovereign funds

- Change is where approved budgets quietly grow. Funders should see change ratio, design-error changes and changes approved in days, by entity and contractor.
- Design-error costs recovered from designers are capital returned to the funder; ask whether the entity tracks them at all.

Adviser's checklist — for consultants recommending project governance

Questions to ask in the diagnostic

- Can the client trace each change order to its cause and its originating RFI?
- Is change priced against the contract schedule of values, or negotiated in correspondence?
- Does the client know how much it has paid for design errors, and has it pursued designers for it?

Recommendations to put in the governance report

- Manage RFIs, change events, PCOs, change orders and claims as one linked chain of records.
- Capture change cause as data and report design-error changes for recovery.
- Profile contractor RFI, claim and change behaviour across the portfolio before each new invitation.

Evidence That Change Controls Are Working

- **Traceability.** Every change order linked to its cause: a change event, PCO, RFI or owner instruction.
- **Contract-rate pricing.** Change line items priced at schedule of values rates unless a variance is approved and explained.
- **Design recovery.** Design-error change value with a corresponding notice or back-charge to the designer.
- **Review time.** High-value change orders no longer approved faster than a genuine review allows.
- **Change ratio.** Approved changes within tolerance by contract, contractor and programme.

Key takeaway

A change order is the end of a story that starts with an RFI, a change event or a bid. When PMWEB links every record in that story, an over-priced change, a design error passed to the owner or a claim strategy is no longer hidden in separate logs.

Filing every letter in a correspondence platform is not the same as controlling change; the cause, value and rate must be data.

The owner sees the whole chain, and so does anyone who reviews it later.

Migrating the change chain to PMWEB turns correspondence into controllable data.

Next in the series: Part 5 turns to payments: how PMWEB progress invoice data exposes abuse of approval power through delayed approvals, unjustified cuts and selective payment release.

Talk to us: If your projects run on Aconex or another document management system, a CDE without DoA-driven workflows, a PMIS without ERP integration or full cost and contract management, or no system at all, there is no longer an excuse to stay: migrate your fraud-exposed processes to a PMIS like PMWEB. CMCS can assess your current platforms and data, start PMWEB on a new programme, integrate it with your ERP and document platforms, and migrate legacy project data, including from Oracle Aconex and Oracle Unifier. Contact CMCS at info@CMCS-MENA.com. Management consultants designing project governance for their clients are welcome to use these frameworks; CMCS works alongside consulting firms to turn governance recommendations into configured PMWEB processes. Ministries of finance and sovereign funds can also see how a common PMWEB standard across funded entities gives them verified, portfolio-wide visibility.

#PMWEB #CMCS #FraudPrevention #ChangeManagement #Claims #RFI #FIDIC #CapitalProjects #ContractAdministration #PMIS #CDE #DocumentManagement #ERPIntegration #ManagementConsulting #ProjectGovernance #MinistryOfFinance #SovereignWealthFund

About the Author

Bassam Samman, PMP, PSP, EVP, GPM is the Chairman and Chief Executive Officer of CMCS FZCO, the PMWEB Authorised Implementation Partner for the Gulf Cooperation Council and broader Middle East and North Africa region. CMCS holds the PMWEB Global Partner of the Year 2025 designation and serves capital project owners, contractors and consultants across the UAE, Saudi Arabia, Qatar and Kuwait.

Bassam has over four decades of experience providing project management, project controls services and project management information systems to more than two hundred capital projects with a combined value exceeding one hundred billion US dollars. He is the author of four published books on project management digitalisation, and has lectured at more than three hundred and fifty international events. He is a co-founder of the Project Management Institute Arabian Gulf Chapter. He holds a Master's degree in Engineering Administration (Construction Management), with Faculty Commendation, from George Washington University and a Bachelor's degree in Civil Engineering from Kuwait University, with executive education at Harvard Business School and London Business School.

About PMWEB

PMWEB is an enterprise-class, web-based capital construction project management platform trusted by organisations worldwide including Harvard University, the United Nations, and Atlanta Airport. Built on Microsoft .NET technology, PMWEB manages the entire project lifecycle within a single integrated platform — from portfolio planning and cost management through document control, procurement, scheduling, asset management, and business intelligence. With 150+ pre-configured SSRS reports, drag-and-drop dashboard design, multi-currency support, and open REST/SOAP API integration, PMWEB delivers enterprise capability with implementation timelines measured in months, not years.

About CMCS

CMCS (Collaboration, Management and Control Solutions) is the PMWEB Authorised Implementation Partner for the GCC and MENA regions and PMWEB Global Partner of the Year 2025, with offices in Dubai, Abu Dhabi and Riyadh. CMCS specialises in digital project management solutions for real estate developers, government entities,

infrastructure owners, project management consultants and construction companies across the Middle East and North Africa.

Payment Integrity — Detecting Abuse of Approval Power on Interim Payment Certificates

Approval days, cuts and payment release as evidence

Late payment is usually treated as an administrative failure. Sometimes it is a lever. The person who can slow an invoice, cut it or hold the payment has power over a contractor's cash flow, and power that is not measured can be sold.

Delayed payment of interim progress invoices causes contractor cash-flow hardship, and hardship becomes claims and disputes. My earlier article on payment fraud made a further point: delay can also be deliberate. Those approving payments can use their "approval power" to pressure a contractor, to favour another, or to extract something in return. This article rewrites and expands that argument and shows how PMWEB turns every invoice into evidence of how each contractor was treated.

Is this article for you?

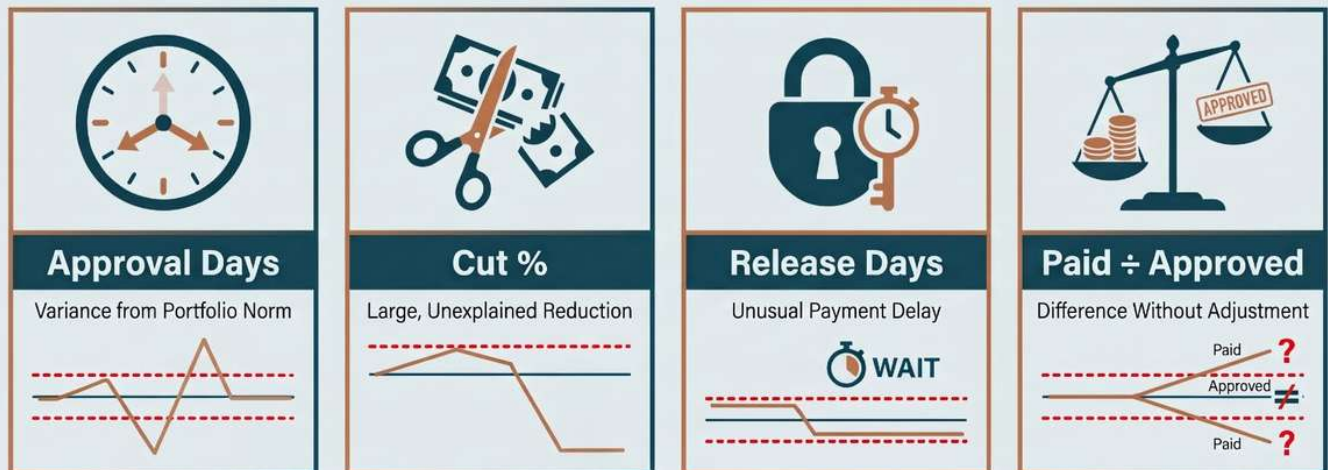
Read this if your payment certificates are approved as **documents in Aconex, a DMS or a CDE** and then keyed into the ERP, if your **PMIS cannot integrate with the ERP**, or if it has **no progress invoice process at line-item level**. If you advise clients on project governance, the adviser's checklist near the end turns this article into diagnostic questions and recommendations. Ministries of finance and sovereign funds will find a funder's lens on this topic near the end.

Four Ways Approval Power Is Abused

Abuse	How it shows up	What it may hide
Delayed approval	One contractor's invoices take far longer to approve than others of similar value and complexity	Pressure for a kickback, or retaliation against a contractor that refused one
Unjustified cuts	The approved amount is cut from the submitted amount well beyond the usual assessment margin	Pressure, or a cut later 'restored' in return for a favour
Delayed payment release	Approved invoices wait an unusually long time before payment	Selective treatment by finance or the approver
Selective partial payment	Paid amount is less than the approved amount without a recorded reason	Off-record negotiation of what will be paid

The opposite pattern matters just as much. Invoices that are approved unusually fast, with almost no cut, for one contractor may indicate favouritism, collusion or payment for work not done.

Four Signals of Payment Abuse



Too slow or too fast — both need an explanation

Every invoice records how a contractor was treated.

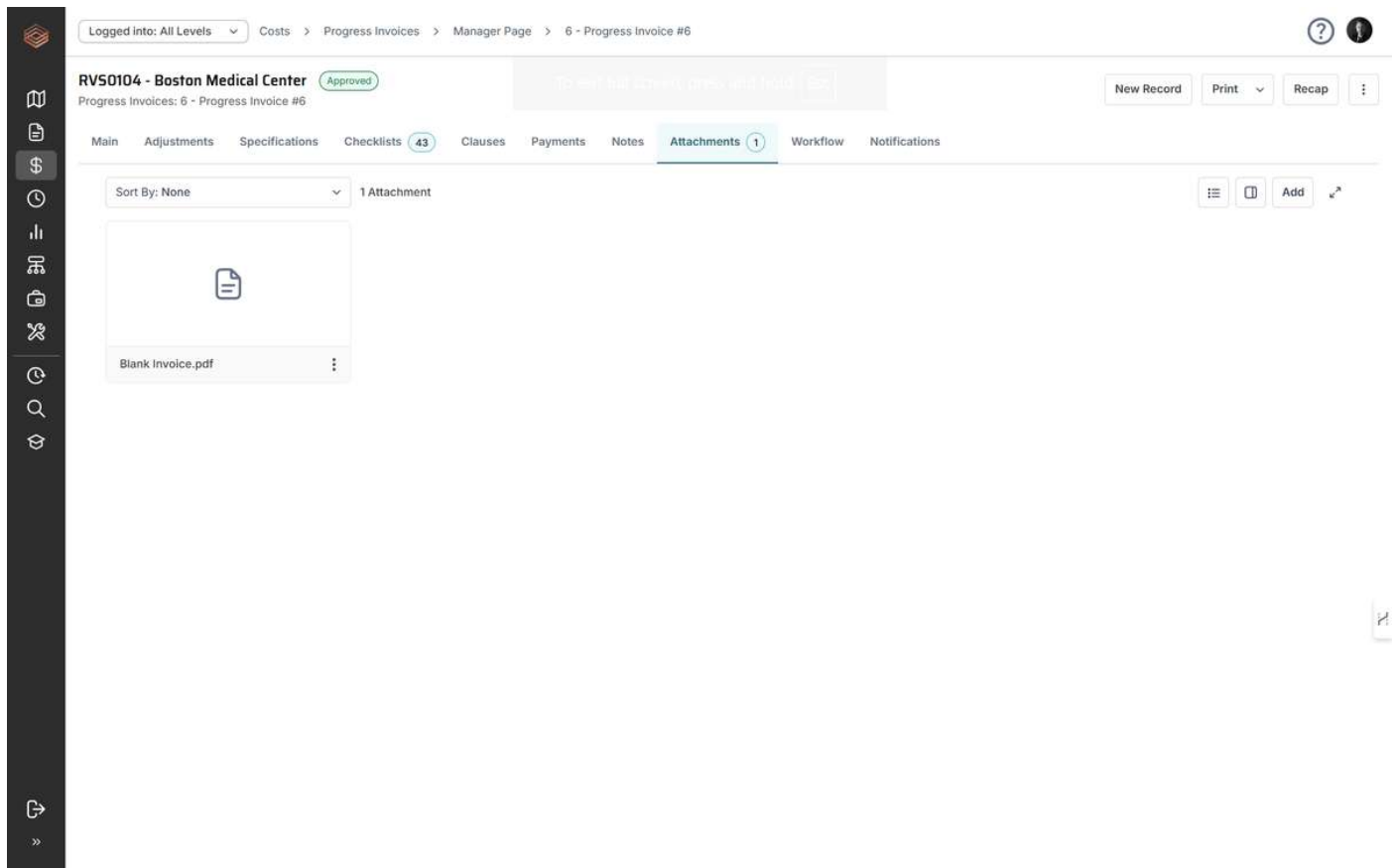
Fair, fast, consistent payment is a fraud control.

CMCS | PMWEB Authorised Implementation Partner - GCC & MENA
Geminis Notebook

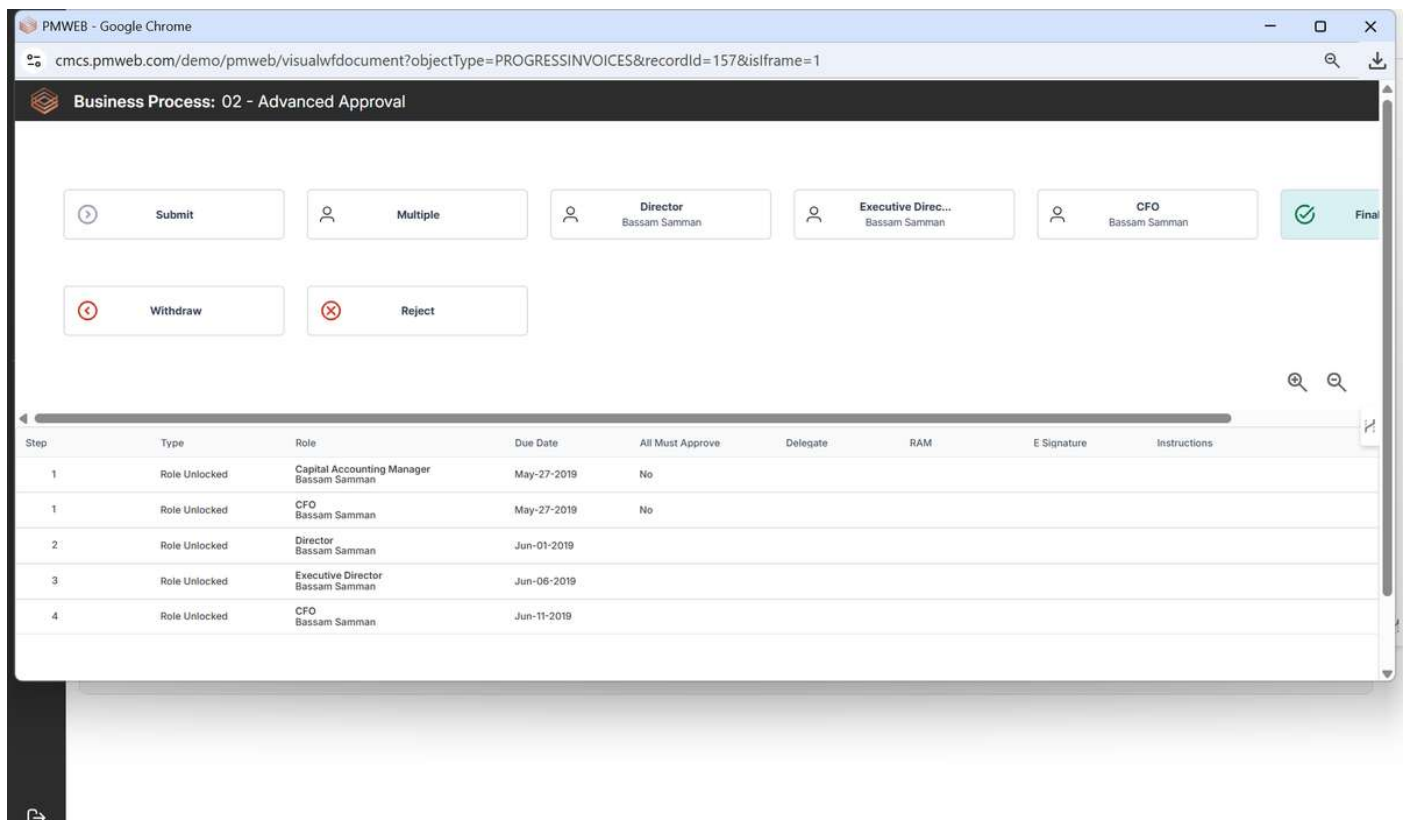
Capturing Every Invoice at the Granular Level

To find exceptions, the owner needs every interim progress invoice submitted, approved and paid against every contract and purchase order across the whole portfolio. In PMWEB, the progress invoice module captures this out of the box for each commitment:

- **Submission.** The amount submitted by the contractor or vendor and the submission date.
- **Work in place and stored materials.** Percent complete by line item, based on measured quantities, an estimate of completion or the linked schedule activity's percent complete.
- **Retention.** Calculated automatically on work in place and on stored materials.
- **Approval.** The approved amount for each line and the approval date, from the workflow history.
- **Payment.** The amount actually paid, the payment date and the transfer details.



The workflow maps submission, review and approval, the role for each step, its duration and the available actions. Conditions apply the DoA matrix, because every invoice has a financial consequence and the approval authority depends on its value and the roles involved. The workflow tab records the planned steps and the actual history: date and time, user, action, comments, delegate and whether team input was requested.



Why the ERP Alone Cannot Protect Payments

Finance teams often argue that payments are already controlled because every payment goes through the ERP. The ERP does control what it was designed for: three-way matching of purchase orders, receipts and invoices, payment runs and the general ledger. It was not designed to judge whether a construction progress invoice is right, or whether the people approving it used their power fairly.

- **The ERP does not know what work was done.** It has no measured quantities, percent complete by line item, accepted work inspection requests or stored materials. A progress claim can be over-stated and still pass a three-way match.
- **The certificate is approved somewhere else.** The interim payment certificate is reviewed and signed in a document platform or on paper, then keyed into the ERP. The ERP records when it received the approved amount, not how long the contractor waited or how much was cut.
- **The cut is invisible.** The ERP sees only the approved figure. The difference between what the contractor submitted and what was approved, the clearest signal of abuse of approval power, is never captured.
- **Payment timeliness starts at the wrong date.** ERP reports measure days from invoice entry to payment. The weeks a certificate spent waiting for approval before it reached the ERP do not exist in its data.

This is false assurance at its most expensive, because the ERP's audit reputation is strong. The answer is not to replace the ERP. It is to manage the progress invoice in PMWEB, where submission, line-level assessment, checklist, workflow and inspection links are captured, and to integrate the approved certificate and payment with the ERP so both systems hold the same, traceable figures.

The return on getting this right is measured twice: once in the payments that are not manipulated, and again in the claims for late or under-payment that are never filed.

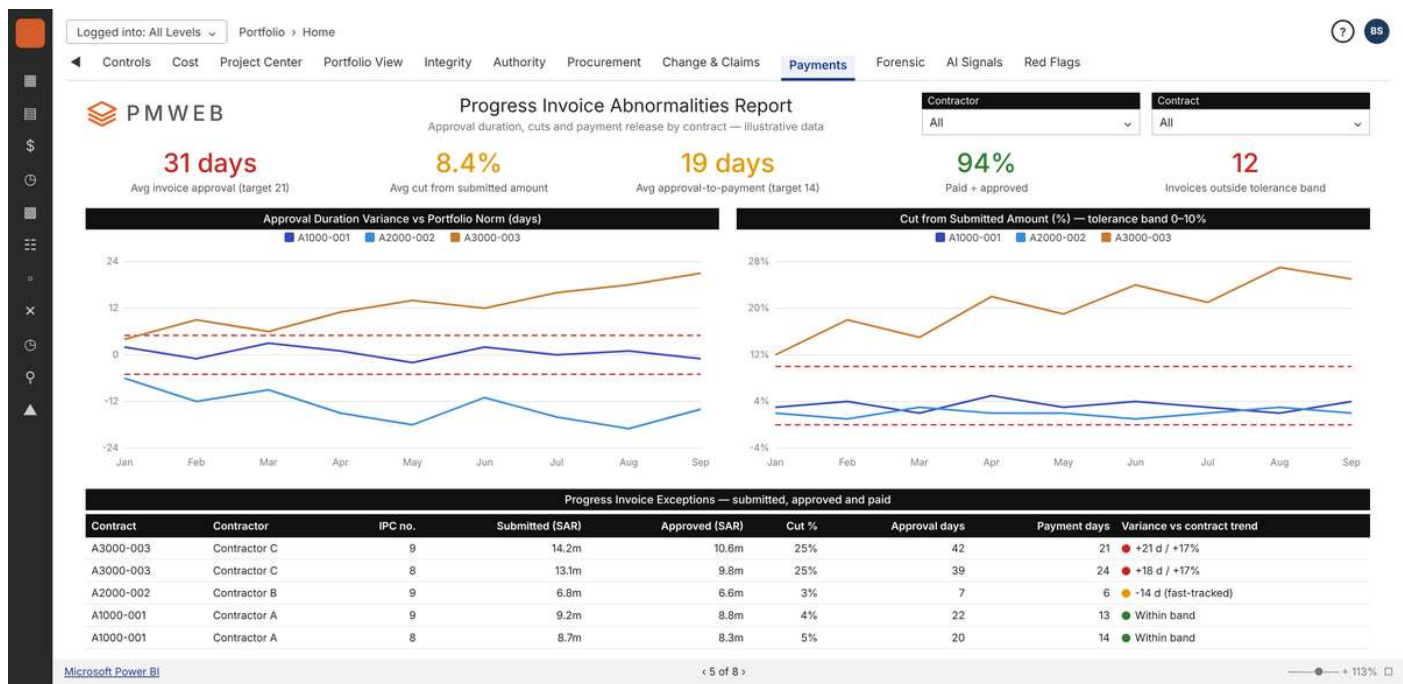
The same gap opens when the PMIS itself cannot be integrated with the ERP. The certificate may be approved properly in the project system, but if finance re-keys it, the approved and paid figures can drift apart without anyone noticing, and a payment can be made that no approved certificate supports. And if the PMIS has no line-level progress invoice process at all, the owner is back to approving PDFs. PMWEB's progress invoices post to its cost ledger and pass to the ERP through its open APIs, so the approved certificate and the payment reconcile by design.

No excuse to stay on the wrong platform

If certificates are approved as documents and re-keyed into the ERP, or your PMIS cannot integrate with it, the most direct route to the owner's money is the least controlled. **Migrating progress invoices to a PMIS like PMWEB, integrated with the ERP**, is where many owners should start their move.

The Progress Invoice Abnormalities Report

With the data in place, a single report shows how each contractor has been treated over time. It plots, for every contract, the variance from the portfolio norm in approval duration, cut percentage, payment release duration and paid-to-approved percentage, against tolerance bands. It filters by contractor and contract, and its log lists every invoice with its submitted, approved and paid amounts and dates.



Progress Invoice Abnormalities Report — Power BI on the PMWEB database, embedded in PMWEB. Illustrative data.

Three contracts tell three stories in the illustrative data. Contract A1000-001 sits inside both tolerance bands: normal treatment. Contract A3000-003 drifts steadily outside them, with approvals now three weeks slower than the norm and a quarter of each invoice cut. Contract A2000-002 is approved two weeks faster than the norm with almost no cut. Neither pattern proves wrongdoing. Both demand an explanation, and the report tells the reviewer exactly which invoices, steps and approvers to ask about.

Payment red flag	Rule on PMWEB data
Slow approval for one contractor	Approval duration above the portfolio norm for its value band by more than N days, for consecutive invoices
Fast-tracked approval	Approval duration far below the norm with near-zero cut, repeatedly on the same contract
Excessive cut	Approved ÷ submitted below the tolerance band without a recorded assessment reason
Held payment	Approval-to-payment days above contract terms or the norm
Paid differs from approved	Paid amount ≠ approved amount without a recorded adjustment
Progress ahead of inspection	Percent complete invoiced on items without accepted work inspection requests
Same approver on outliers	One approver appears on a disproportionate share of outlier invoices

Because invoice data sits with all other PMWEB processes, it can be read alongside them. A contractor whose invoices are slowed may also be the one with a rejected claim or a refused change order. A contractor whose invoices are fast-tracked may also be the one whose change orders are approved in days. The correlation is often more revealing than either pattern alone.

Funding Release Against Verified Progress

For a government entity, the progress invoice is not the end of the chain. The entity requests funds from the ministry of finance; a project company draws on its investors or lenders. If those requests are assembled outside the project system, the funder releases capital against a summary, and every weakness described above is passed upwards. In PMWEB, budgets and commitment lines carry their funding source, and approved progress invoices carry the certified value of work in place. A funding request can then be built from approved certificates and commitments, traceable line by line, and the funder can see exactly which certified work each release pays for.

Logged into: All Levels > Costs > Commitments > Manager Page > 002 - GMP Contract

RV50104 - Boston Medical Center Submitted (Step 1 of 2)

Commitments: 002 - GMP Contract

New Record Print Recap

Main Adjustments Specifications Clauses 3 Change Orders 3 Progress Invoices 9 Payments Notes Attachments 79 Workflow Step 1 of 2 Notifications

Currency* USD - Dollar (United States of Am... Type Subcontract Category Reference

WBS : Expiration Date 30-Sep-2011 12:00:00 tt Days 730.00 Procurement #

Status Submitted Revision 0 Use Units Paid In Full

User Defined Fields

Contract Mgr Original Completion Revised Completion Projected Completion

Actual Completion Work Package test delete \$0.00

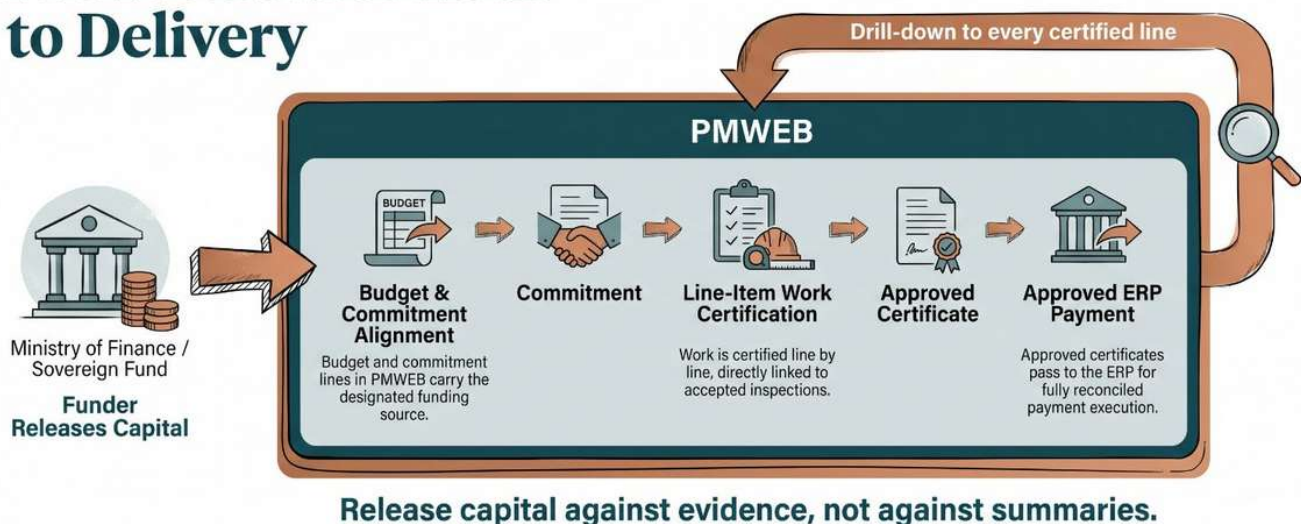
Billing And Shipping

Details

Group by: None Layout: Dubai Police Export To Excel Preview Conversions

Attach...	Cost Code	Description	UOM	Quantity	Unit C...	Currency	Ext. C...	Adjust...	Total ...	Cost Period	WBS
[Q]	02-010002 - Gener...	General Conditions		2	\$100,000.00	USD - Dollar (United States of America)	\$200,000.00	\$0.00	\$200,000.00	*Split*	
[Q]	02-020000 - Existi...	Existing Conditions		0.09	\$1,000,000.00	USD - Dollar (United States of America)	\$90,000.00	\$0.00	\$90,000.00	*Split*	
[Q]	02-030000 - Concr...	Concrete		8	\$425,000.00	USD - Dollar (United States of America)	\$3,400,000.00	\$0.00	\$3,400,000.00	*Split*	

From Disbursement to Delivery



Without a PMIS: release against a spreadsheet request

Disbursement is the funder's last control point.

CMCS | PMWEB Authorised Implementation Partner - GCC & MENA
Gemini Notebook

Where PMWEB 2026 AI Helps

Payment reviews are a natural fit for the PMWEB 2026 AI Assistant's find and open modes. A commercial director can ask it to find all progress invoices on a contract where approved is less than 85% of submitted, open the most recent one and see its workflow log, or find every invoice approved by a given role in under two days this quarter. Where follow-up is needed, the assistant creates the red flag or a query to the approver once the reviewer approves. Spotting a

slow drift across dozens of contracts and hundreds of invoices, before it becomes obvious on a chart, is the job of the analytics described in Part 7.

Email, ERP and PMWEB Invoice Control Compared

Capability	Invoices by email and finance system	ERP with document-platform approval	Progress invoices in PMWEB
Submission date	Disputed	Upload date of a PDF, or ERP entry date	Recorded on submission
Completeness	Argued after the fact	Not checked against inspections or measured work	Checklist completed before submission
Assessment	Cut without a line-level record	Approved total keyed into ERP; line detail and cut lost	Approved amount by line with reasons
Approval authority	Signature on the certificate	Document stamp, then ERP approval: two records that can differ	Workflow with DoA rules and history
Payment	In finance, separate from the certificate	Paid in ERP against an invoice number only	Payment recorded against the approved invoice
Treatment across contractors	Invisible	Payment timing visible; approval delay and cuts invisible	Compared by contractor, contract and approver

The funder's lens — ministries of finance and sovereign funds

- Disbursement is the funder's last control point. Release funds against certificates approved in a PMIS and reconciled to the ERP, not against payment requests assembled outside it.
- Payment-treatment indicators reveal whether contractors are paid fairly. Unfair payment becomes claims, and claims become cost the funder ultimately bears.

Adviser's checklist — for consultants recommending project governance

Questions to ask in the diagnostic

- Is the interim certificate assessed line by line in a project system, or approved as a PDF and keyed into the ERP?
- Can the client show approval days, cut percentage and release days for every contractor?
- Do approved and paid figures reconcile through integration?

Recommendations to put in the governance report

- Manage progress invoices in the PMIS with a submission checklist and DoA workflow.
- Integrate approved certificates and payments with the ERP to remove re-keying.
- Add payment-treatment indicators by contractor and approver to the PMO dashboard.

Evidence That Payment Controls Are Working

- **Cycle time.** Average and spread of invoice approval days within target, by programme and contractor.
- **Consistency.** Narrowing gap between the fastest and slowest treated contractors for similar invoices.
- **Explained cuts.** Every cut beyond the tolerance band has a recorded assessment reason.
- **Payment discipline.** Approved invoices paid within contract terms; paid equals approved unless explained.
- **Fewer payment claims.** Contractor claims citing late or under-payment falling over time.

Key takeaway

Every invoice records how a contractor was treated: how long it waited, how much was cut and when it was paid. PMWEB captures those facts for every contract, so abuse of approval power shows up as a pattern rather than a rumour.

The ERP controls the payment run, not the certificate behind it; without the progress invoice in a PMIS, abuse of approval power never reaches the ledger.

Fair, fast and consistent payment is a fraud control, and it is also the cheapest way to avoid claims.

Progress invoices are often the right first process to migrate to PMWEB.

Next in the series: Part 6 looks backwards: how a forensic audit team can rebuild a project's financial record in PMWEB to identify the parties behind fraudulent activities and support recovery of lost funds.

Talk to us: If your projects run on Aconex or another document management system, a CDE without DoA-driven workflows, a PMIS without ERP integration or full cost and contract management, or no system at all, there is no longer an excuse to stay: migrate your fraud-exposed processes to a PMIS like PMWEB. CMCS can assess your current platforms and data, start PMWEB on a new programme, integrate it with your ERP and document platforms, and migrate legacy project data, including from Oracle Aconex and Oracle Unifier. Contact CMCS at info@CMCS-MENA.com. Management consultants designing project governance for their clients are welcome to use these frameworks; CMCS works alongside consulting firms to turn governance recommendations into configured PMWEB processes. Ministries of finance and sovereign funds can also see how a common PMWEB standard across funded entities gives them verified, portfolio-wide visibility.

#PMWEB #CMCS #FraudPrevention #ProgressInvoices #PaymentCertificates #CashFlow #CapitalProjects
#ContractAdministration #PMIS #Integrity #CDE #DocumentManagement #ERPIntegration #ManagementConsulting
#ProjectGovernance #MinistryOfFinance #SovereignWealthFund

About the Author

Bassam Samman, PMP, PSP, EVP, GPM is the Chairman and Chief Executive Officer of CMCS FZCO, the PMWEB Authorised Implementation Partner for the Gulf Cooperation Council and broader Middle East and North Africa region. CMCS holds the PMWEB Global Partner of the Year 2025 designation and serves capital project owners, contractors and consultants across the UAE, Saudi Arabia, Qatar and Kuwait.

Bassam has over four decades of experience providing project management, project controls services and project management information systems to more than two hundred capital projects with a combined value exceeding one hundred billion US dollars. He is the author of four published books on project management digitalisation, and has lectured at more than three hundred and fifty international events. He is a co-founder of the Project Management Institute Arabian Gulf Chapter. He holds a Master's degree in Engineering Administration (Construction Management), with Faculty Commendation, from George Washington University and a Bachelor's degree in Civil Engineering from Kuwait University, with executive education at Harvard Business School and London Business School.

About PMWEB

PMWEB is an enterprise-class, web-based capital construction project management platform trusted by organisations worldwide including Harvard University, the United Nations, and Atlanta Airport. Built on Microsoft .NET technology, PMWEB manages the entire project lifecycle within a single integrated platform — from portfolio planning and cost management through document control, procurement, scheduling, asset management, and business intelligence. With 150+ pre-configured SSRS reports, drag-and-drop dashboard design, multi-currency support, and open REST/SOAP API integration, PMWEB delivers enterprise capability with implementation timelines measured in months, not years.

About CMCS

CMCS (Collaboration, Management and Control Solutions) is the PMWEB Authorised Implementation Partner for the GCC and MENA regions and PMWEB Global Partner of the Year 2025, with offices in Dubai, Abu Dhabi and Riyadh. CMCS specialises in digital project management solutions for real estate developers, government entities,

infrastructure owners, project management consultants and construction companies across the Middle East and North Africa.

Forensic Audit in PMWEB — Rebuilding the Record to Recover Lost Funds

Turning scattered project files into evidence an investigation can rely on

Money lost to fraud on a capital project is usually written off as a sunk cost. It does not have to be. A forensic audit can identify who was involved and support recovery, but only if the project's records can be assembled into a form that can be analysed, compared and trusted.

Parts 1 to 5 of this series described controls that prevent and detect fraud while a project is running. Many owners, however, face the opposite situation: a completed or troubled project, delivered on paper, spreadsheets and email, where something has clearly gone wrong. This article rewrites my earlier article on forensic audits and shows how PMWEB can be used as the audit team's workbench, even when the project was never managed in it.

Is this article for you?

Read this if your project records sit in **Aconex, a DMS, a CDE or shared drives**, with the money in the ERP and the analysis in spreadsheets, and an audit would first have to rebuild the transactions from PDFs. If you advise clients on project governance, the adviser's checklist near the end turns this article into diagnostic questions and recommendations. Ministries of finance and sovereign funds will find a funder's lens on this topic near the end.

Forensic audit is the last line of defence, not the first. By the time it starts, the money has been paid and recovery depends on lawyers, time and the willingness of the parties involved. It is also where the cost of silence becomes visible: in most cases, someone had suspected the problem long before the audit, but nobody had the mandate, the data or the courage to raise it. Recovering funds is valuable. Preventing the loss would have been worth far more, and the same PMWEB record that supports a forensic audit is what makes prevention possible on the next project.

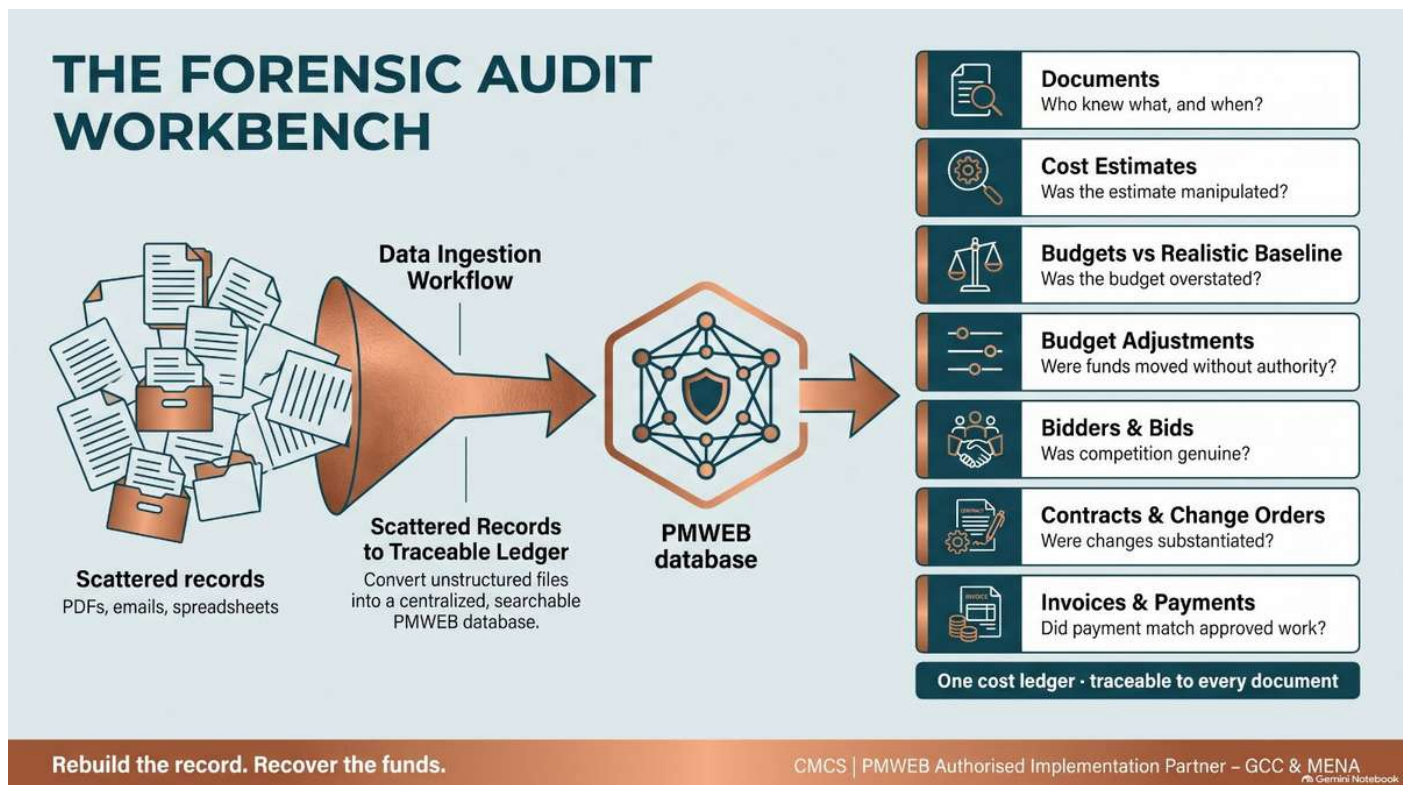
Compare the economics. A forensic audit and the legal action that follows it can cost a significant share of the amount eventually recovered, and many losses are never recovered at all. A PMIS that prevents the same losses costs a fraction of the capital it protects and keeps protecting it on every project that follows.

The Forensic Challenge Is a Data Challenge

A forensic audit succeeds or fails on the availability of data in a format that allows analysis. At a minimum the team needs:

Record set	What the audit tests
Approved cost estimates and their revisions	Whether the estimate was manipulated to justify a budget or an award
Baseline budget and budget adjustments	Whether funds were moved without reason or authority
Invited bidders, bid analysis and technical evaluation	Whether competition was genuine and bidders were qualified
Awarded contracts and their terms	Whether the contract matches what was evaluated and approved
Interim payment certificates and payments	Whether payments match work done and approved amounts
Approved and disputed change orders	Whether changes were substantiated and fairly priced
RFIs, site work instructions, meeting minutes	Who knew what, and when

Findings often widen the scope to substituted materials and equipment, testing and commissioning inspections, and punch lists. Each of these is easier to examine when it sits in a structured record rather than a scanned file.



Rebuilding the Record in PMWEB

PMWEB's out-of-the-box modules for document management, cost estimate, budget, budget requests, vendor prequalification, bid comparison, commitments, progress invoices, miscellaneous invoices and change orders give the audit team a ready-made structure. The work is to load the evidence into it, in this order.

1. Documents

All documents in scope are scanned into searchable files and uploaded to PMWEB document management, in folders and subfolders that organise and secure them, for example project contracts, procurement, cost information, correspondence, memoranda and construction claims by type. Attributes capture additional data on each document. The markup viewer lets auditors highlight and annotate key passages. Because the files are searchable, the team can search their content for key events, and each document can be attached to the PMWEB records it supports.

Logged into: All Levels Tools > Document Manager > Manager Page > Go to Manager Page

033000 Cast In Place Concrete

Document Manager > Projects > RV50104 - Boston Medical Center > 11 Design Stage > 114 Construction Documents > 11402 Specification > 03 Concrete > 033000 Cast In Place Concrete

Folders

- Document Manager Root Folder
 - Projects
 - DEMO-Tec01 - Demo Funcional Tec
 - EOI Documents
 - P02 - Shreyaswi
 - P03 - Sai (Test)
 - P04 - Reshma
 - Project 01 - TEST 01(internal)
 - PV0050 - Boston Medical Center(1)
 - RV50104 - Boston Medical Center
 - 11 Design Stage
 - 111 Concept
 - 112 Schematic
 - 113 Design Development
 - 114 Construction Documents
 - 11401 General Discription
 - 11402 Specification
 - 03 Concrete
 - 033000 Cast In ...
 - 04 Masonry
 - 07 Thermal and Moistur...
 - 11403 Site
 - 11404 Landscaping
 - 11405 Structural
 - 11406 Building Exterior Env...
 - 11407 Building Interior

Search in Document Manager.... Advanced Search

Sort By: Name 1 Selected

Files

- 1124 - 033000 Cast In P...
- 1277 - A-1500-A(13).pdf
- 1276 - A-1500-A(5).pdf
- 1275 - A-1501-A(11).pdf
- 1274 - A-1501-A(12).pdf
- 1273 - A-1501-A(5).pdf
- 1272 - A-1502-A(11).pdf
- 1271 - A-1502-A(12).pdf
- 1270 - A-1502-A(5).pdf
- 1278 - Building.jpg

1278 - Building.jpg

Description
Building

Type

Category

Version
1

Status
Draft

Geolocation

Attributes
Building

Unifomat

Masterformat

Building Level

2. Cost estimates

Every estimate revision, including the final approved estimate, is captured in the cost estimate module. Where estimates exist in Excel they are imported; where they exist only on paper they are first converted to a structured Excel file. The team can then compare revisions line by line and see what changed, when, and how each change affected the approved budget.

3. Budgets: approved versus realistic

The audit team uses the final approved estimate to build a realistic baseline budget, and captures every budget the project actually used, including the approved baseline, in the budget module. Budgets can be pasted in directly to save time. Comparing the approved baseline with the realistic baseline shows where the budget was overstated and by how much.

4. Budget adjustments

Every omission, addition and transfer applied to the baseline is captured as a budget request, with its reason, requester, approver, scope and date. Transfers out of contingency, and transfers made shortly before or after a large commitment or change order, receive particular attention.

5. Bidders and bids

The invited bidders for each package are captured in the vendor prequalification module and scored on financial capacity, track record, conflict of interest and other criteria, to establish whether they should have been invited. Their bids are captured in the procurement module against the approved estimate, which immediately exposes unbalanced items and front-loading, as described in Part 3. Technical evaluations are captured where available.

6. Contracts, change orders, invoices and payments

Each awarded contract is captured as a commitment with its terms and bill of quantities, pasted from Excel. Approved and disputed change orders are captured with the line items they affect and any time extension. Each interim payment certificate is captured as a progress invoice with percent complete, stored materials, amount approved and amount paid, with dates. All other project expenses, such as site storage, permits and authority fees, are captured as miscellaneous invoices.

Why "It Is All in the System" Rarely Helps an Audit

Forensic teams increasingly hear that the project was fully digital, so the evidence will be easy to find. In practice, when the project ran on a document platform, an ERP and spreadsheets, the audit faces almost the same task as a paper project. The documents are searchable, but the figures inside them are not data. The ERP ledger shows payments, but not the estimate, the bids, the pending changes or the work in place behind them. The platform's logs show who opened a file, not who approved which amount under which authority.

Worse, the belief that everything was digital may have delayed the audit itself. Management assumed the system would have caught problems, so nobody looked until the losses were too large to ignore. That is the real cost of false assurance: it does not only let fraud through, it postpones its discovery. Rebuilding the record in PMWEB, as described above, converts documents back into transactions so they can be tested.

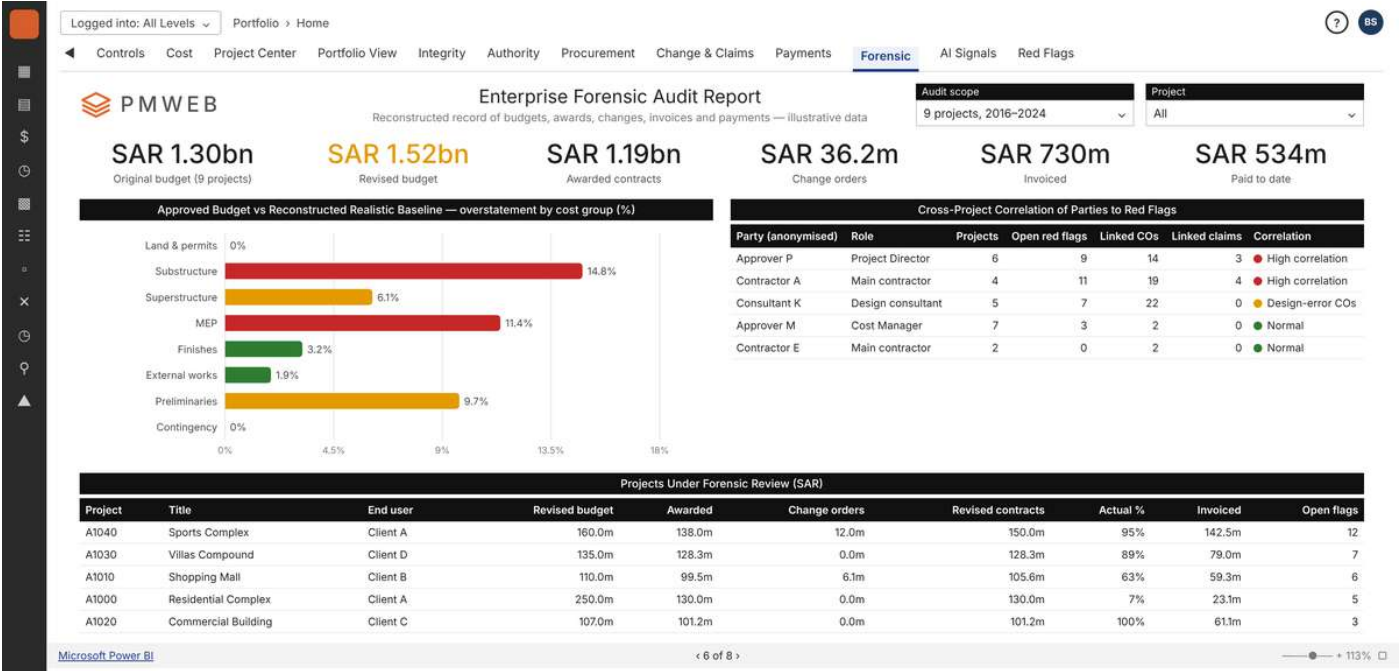
No excuse to stay on the wrong platform

If a forensic review would have to rebuild your records from PDFs, the same will be true of the next one.
Migrating to a PMIS like PMWEB now, starting with new programmes and bringing live projects across in waves, means the next audit tests controls instead of reconstructing transactions.

Analysis and Reporting

With the record rebuilt and trustworthy, the team analyses it with Power BI on the PMWEB database. Variances between approved and realistic baselines, awards against estimates, change orders against contract rates, and payments against approved work identify the transactions that need detailed examination. Scorecards and visuals help communicate findings to the board, investigators and legal advisers.

Because PMWEB holds an unlimited number of projects and programmes, the owner can consolidate the results of several audits on one dashboard. That is where correlations appear: the same individuals or companies across troubled projects, the same period, the same project type, the same approver.



Enterprise Forensic Audit Report — Power BI on the PMWEB database, embedded in PMWEB. Illustrative data; parties anonymised.

In the illustrative report, substructure and MEP budgets were overstated by 15% and 11% against the reconstructed realistic baseline. The correlation table shows one approver and one main contractor appearing together on several projects carrying most of the open red flags and linked change orders, and a design consultant associated with an unusual number of design-error changes. These are the leads an investigation follows, record by record, before any conclusion is drawn.

Forensic Red Flags

Red flag	Rule on rebuilt PMWEB data
Overstated baseline	Approved baseline above realistic baseline by cost group beyond tolerance
Contingency drained early	Transfers out of contingency concentrated before large awards or changes
Estimate revised to fit a bid	Estimate revision approved between bid opening and award
Awarded rates differ from evaluated rates	Commitment schedule of values rates differ from the evaluated bid
Paid without approved certificate	Payment with no matching approved progress invoice
Duplicate or split invoices	Same vendor, amount and description across invoices or projects
Recurring party combinations	Same approver, contractor and consultant across multiple flagged projects

Where PMWEB 2026 AI Helps

Forensic teams spend much of their time looking for things. Once the record is rebuilt, the PMWEB 2026 AI Assistant lets an auditor find records in plain language, such as every change order on a project approved by a given role in a given year, every budget transfer out of contingency above a threshold, or every invoice from a vendor across all audited projects, and open them directly. With the auditor's approval it can create findings as records linked to the evidence. Because it honours PMWEB security settings, sensitive investigation records remain restricted to the audit team. Part 7 explains how analytics can then scan the whole rebuilt record for patterns the team has not yet thought to look for.

Box Files, Non-PMIS Data and a Rebuilt PMWEB Record

Capability	Audit from files and spreadsheets	Data left in a CDE, ERP and spreadsheets	Audit on a rebuilt PMWEB record
Document search	Manual reading	Searchable files, figures still inside PDFs	Full-text search across scanned, attributed documents
Financial reconstruction	Spreadsheets stitched together	ERP ledger without estimate, bids, changes or work in place	Transactions posted to one cost ledger with source links
Bid analysis	Recalculated by hand	Bids as attachments in a closed tender event	Bids compared against the estimate line by line
Cross-project view	One audit at a time	One archive per project	Consolidated findings and correlations across projects
Evidence chain	Copied extracts	File-level links, not transaction links	Each figure traced to its record and document
Prevention	Report filed, lessons forgotten	Same tools, same blind spots on the next project	Same platform used to run future projects under control

The funder's lens — ministries of finance and sovereign funds

- When a forensic review is needed in a funded entity, the funder's priority is recovery and prevention elsewhere. Rebuilding the record in a PMIS shared across entities serves both.
- Cross-entity correlation, the same contractors, consultants or approvers appearing in troubled projects, is only visible to the party that funds them all.

Adviser's checklist — for consultants recommending project governance

Questions to ask in the diagnostic

- If an audit started tomorrow, could the evidence be tested as transactions, or would it first be rebuilt from PDFs?
- Do audit plans test whether controls are enforced by systems, or only whether policies exist?

Recommendations to put in the governance report

- Shift internal audit from sampling transactions to testing system-enforced controls and red-flag dispositions.
- Where a forensic review is needed, rebuild the record in the PMIS that will run future projects.

Evidence That the Forensic Effort Is Working

- **Record coverage.** Share of in-scope documents and transactions captured and linked in PMWEB.
- **Reconciliation.** Rebuilt ledger reconciled to the finance system's payments.
- **Findings substantiated.** Each finding supported by linked records and documents.
- **Recovery pursued.** Value of findings referred for recovery, back-charge or legal action.
- **Controls adopted.** Future projects on the same programme run in PMWEB with the controls from Parts 1 to 5.

Key takeaway

A forensic audit is only as strong as the record it rests on. Rebuilding that record in PMWEB gives the audit team searchable documents, a traceable cost ledger and a portfolio-wide view of who was involved where.

"It was all digital" often means the evidence exists but cannot be tested, and the belief that systems were watching delayed the audit itself.

The same platform then runs the next project under the controls that would have prevented the loss.

Recovery is the last line of defence. The record that supports the audit is the same record that prevents the next loss.

Migrating now means the next audit tests controls instead of rebuilding records.

Next in the series: Part 7 brings the series together: how PMWEB 2026 AI, analytics and machine learning built on structured PMWEB data move fraud detection from periodic review to continuous signals.

Talk to us: If your projects run on Aconex or another document management system, a CDE without DoA-driven workflows, a PMIS without ERP integration or full cost and contract management, or no system at all, there is no longer an excuse to stay: migrate your fraud-exposed processes to a PMIS like PMWEB. CMCS can assess your current platforms and data, start PMWEB on a new programme, integrate it with your ERP and document platforms, and migrate legacy project data, including from Oracle Aconex and Oracle Unifier. Contact CMCS at info@CMCS-MENA.com. Management consultants designing project governance for their clients are welcome to use these frameworks; CMCS works alongside consulting firms to turn governance recommendations into configured PMWEB processes. Ministries of finance and sovereign funds can also see how a common PMWEB standard across funded entities gives them verified, portfolio-wide visibility.

#PMWEB #CMCS #ForensicAudit #FraudRecovery #FraudPrevention #CapitalProjects #CostManagement #PowerBI #PMIS #Integrity #CDE #DocumentManagement #ERPIntegration #ManagementConsulting #ProjectGovernance #MinistryOfFinance #SovereignWealthFund

About the Author

Bassam Samman, PMP, PSP, EVP, GPM is the Chairman and Chief Executive Officer of CMCS FZCO, the PMWEB Authorised Implementation Partner for the Gulf Cooperation Council and broader Middle East and North Africa region. CMCS holds the PMWEB Global Partner of the Year 2025 designation and serves capital project owners, contractors and consultants across the UAE, Saudi Arabia, Qatar and Kuwait.

Bassam has over four decades of experience providing project management, project controls services and project management information systems to more than two hundred capital projects with a combined value exceeding one hundred billion US dollars. He is the author of four published books on project management digitalisation, and has lectured at more than three hundred and fifty international events. He is a co-founder of the Project Management Institute Arabian Gulf Chapter. He holds a Master's degree in Engineering Administration (Construction Management), with Faculty Commendation, from George Washington University and a Bachelor's degree in Civil Engineering from Kuwait University, with executive education at Harvard Business School and London Business School.

About PMWEB

PMWEB is an enterprise-class, web-based capital construction project management platform trusted by organisations worldwide including Harvard University, the United Nations, and Atlanta Airport. Built on Microsoft .NET technology, PMWEB manages the entire project lifecycle within a single integrated platform — from portfolio planning and cost management through document control, procurement, scheduling, asset management, and business intelligence. With 150+ pre-configured SSRS reports, drag-and-drop dashboard design, multi-currency support, and open REST/SOAP API integration, PMWEB delivers enterprise capability with implementation timelines measured in months, not years.

About CMCS

CMCS (Collaboration, Management and Control Solutions) is the PMWEB Authorised Implementation Partner for the GCC and MENA regions and PMWEB Global Partner of the Year 2025, with offices in Dubai, Abu Dhabi and Riyadh. CMCS specialises in digital project management solutions for real estate developers, government entities, infrastructure owners, project management consultants and construction companies across the Middle East and North Africa.

From Red Flags to AI — How PMWEB 2026 and Analytics Detect Fraud Patterns Across the Portfolio

No structured data, no AI: why the controls in Parts 1 to 6 are what make machine detection possible

Rules find the fraud you already know how to describe. Machine learning finds the patterns you have not yet thought to look for. Neither works on emails, scanned letters and spreadsheets. Both work on the structured, approved, linked transactions a PMIS like PMWEB captures every day.

This final part rewrites and updates my earlier article asking whether machines can be trained to detect fraudulent transactions on capital construction projects. The answer then was yes, provided the business processes are digitised. Since then, two things have changed. PMWEB 2026 has introduced an AI Assistant inside the platform, and AI tools that read PMWEB data directly have become practical for owners to deploy. This article explains what each layer does today, what it needs, and how to adopt it responsibly.

Is this article for you?

Read this if you are being offered **AI features on a document platform or CDE** as the answer to fraud detection, or if your **PMIS lacks the cost and contract data and ERP integration** that fraud models need. If you advise clients on project governance, the adviser's checklist near the end turns this article into diagnostic questions and recommendations. Ministries of finance and sovereign funds will find a funder's lens on this topic near the end.

Why Rules Alone Are Not Enough

The red-flag rules in Parts 1 to 6 are essential. They are transparent, easy to explain and cheap to run. But they have limits. Each rule tests one condition that someone already thought of. Fraudsters adapt to known thresholds, for example by splitting a change just below a DoA limit. And the most revealing patterns often span several processes: a contractor that bids low, raises many RFIs, files frequent claim notices and ends its projects in disputes looks unremarkable in any single log.

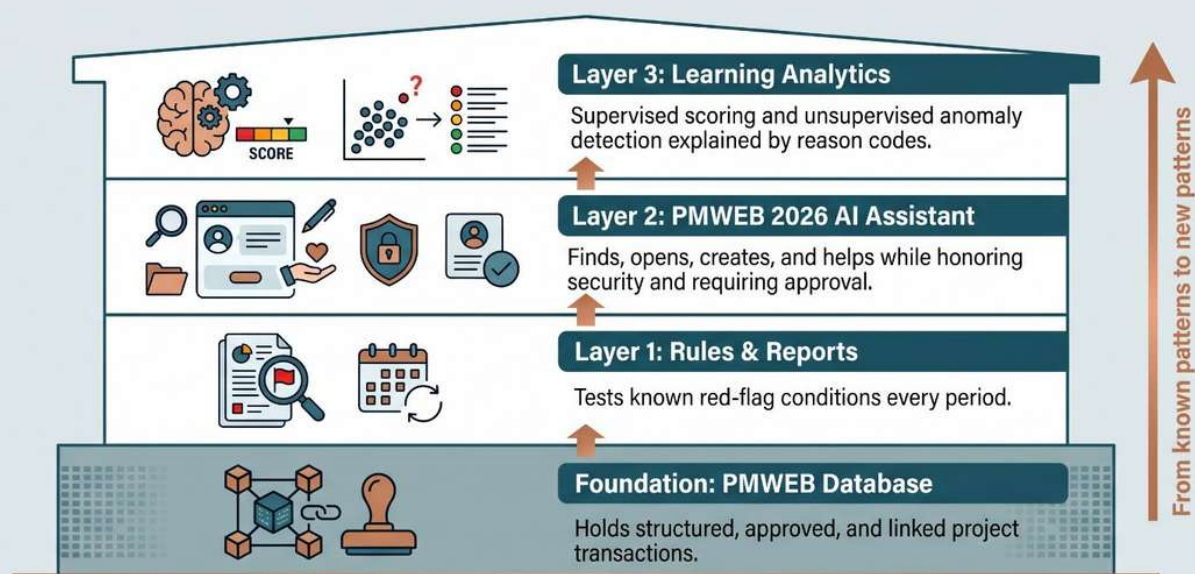
There is also a difference in timing. A periodic audit tests a sample, months later. Rules and analytics on PMWEB data test every transaction, every period, while the contract is still live and the payment can still be stopped. That turns detection from a historical exercise into an active control.

Analytics that learn from the data, rather than from a list of rules, can examine every transaction against every other and highlight combinations no rule describes. They need one thing above all: a large volume of clean, structured, trustworthy transactions.

Three Layers of Fraud Detection on PMWEB Data

Layer	What it does	Available through
1. Rules and reports	Tests known red-flag conditions every period and presents exceptions on dashboards	PMWEB reports and Power BI on the PMWEB database — available today
2. AI Assistant	Lets reviewers find, open and create records and get help in plain language, within their security rights	PMWEB 2026 AI Assistant — inside PMWEB
3. Learning analytics	Scores transactions for risk, finds anomalies and associations, and explains why	Analytics and machine learning on PMWEB data, and AI assistants that read PMWEB through secure connectors such as askAIRO from CMCS

Three Layers of Fraud Detection on PMWEB Data



AI does not replace controls. It depends on them.

No structured data, no AI.

CMCS | PMWEB Authorised Implementation Partner – GCC & Gemini Notebook

Layer 2: The PMWEB 2026 AI Assistant

The PMWEB 2026 AI Assistant works inside the platform in four modes. For integrity and audit work, each mode removes friction from the review.

Mode	What it does	Integrity use case
Find	Locates records from a plain-language request	"Find change orders above SAR 1 million on Mountain Destination approved in under three days this year"
Open	Opens the record or list the user asks for	Open the change order with the largest value and its workflow log
Create	Creates new records from the user's request, with the user's approval	Create an Integrity Red Flag linked to the change order, assigned to internal audit
Help	Explains PMWEB functions, screens and configured processes	Explain the workflow and DoA branches that apply to change orders on this programme

Two design principles matter for integrity work. Actions are taken only with the user's approval, so the assistant never changes a record on its own initiative. And the assistant honours PMWEB security settings, so it can only reveal the projects, modules and fields the user's role allows. An AI that ignored those settings would itself be a fraud risk.

The screenshot displays the PMWEB application interface. The main window shows a form for project 'RV50104 - Boston Medical Center' with various fields for RFI details, including Project#, Description, Phase, WBS, Reference, From, To, Category, Trade, CSI Code, Task, RFI Date, Date Required, Date Answered, Status, Revision, User Assigned, User Due Date, Priority, Change Event, and User Defined Fields. The AI Assistant sidebar on the right provides a summary of open RFIs in the Boston Medical Center project, listing details for RFI #004, RFI #RV50104-ALQ-AJC-006, RFI #007, and RFI #008.

PMWEB's AI roadmap places capabilities such as risk identification in later releases. The approach in this article does not depend on them: owners can start with layers 1 and 2 now and build layer 3 on the same data.

Layer 3: Learning Analytics on PMWEB Data

Machine learning refers to techniques that learn patterns in data without a human analyst specifying them. Two families matter for fraud detection, and both should be used.

Supervised models learn from past outcomes

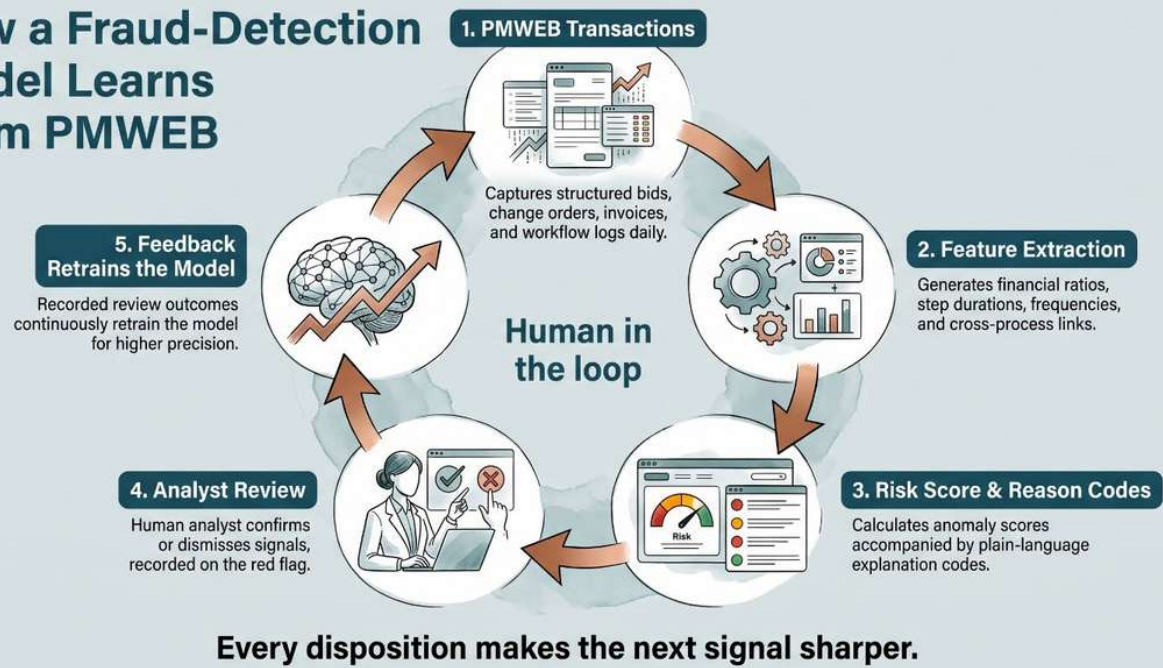
A supervised model is trained on transactions tagged as fraud or not fraud, and learns the patterns that distinguish them. Its accuracy depends directly on the amount of clean, relevant, tagged training data. This is where the Integrity Red Flag record from Part 1 pays off a second time. Every flag that is investigated and closed with a disposition of confirmed or dismissed becomes a tagged example. Over time, the owner's own review history becomes the training set. Typical algorithms include logistic regression, decision trees, random forests, gradient boosting and neural networks; data scientists choose among them based on the volume of data and the need for explanation.

Unsupervised models find what nobody tagged

Where tagged examples are scarce, as they are in most organisations at the start, unsupervised models surface unusual behaviour on their own. Clustering methods such as k-means group similar contractors, contracts or approvers and show which ones sit far from their group. Anomaly detection highlights transactions unlike any others of their type. Association methods such as the Apriori algorithm find combinations that occur together more often than chance, such as a particular approver, consultant and contractor.

My original article gave an example that remains the best illustration. An unsupervised model notices that one contractor raises unusually large volumes of RFIs and claim notices on every project it has with the owner. Its prequalification submission shows pending claims with other owners. The bid comparison history shows it always bids lowest. Together these suggest a claim-oriented contractor that relies on claims to recover margin. No single rule would have joined those facts; the combined pattern did.

How a Fraud-Detection Model Learns From PMWEB



A score is a question, not an accusation.

CMCS | PMWEB Authorised Implementation Partner – GCC & MENA

Gemini Notebook

What the models learn from

Every process digitised in PMWEB adds features the models can use. The more processes, projects and years in the database, the better they perform.

PMWEB process	Example features for fraud models
Vendor prequalification	Company age at invitation, score, pending claims declared, shared directors or addresses
Bid comparison	Line-item ratio to estimate, spread across bidders, rank history, front-loading index
Commitments	Award versus estimate, rates by item, retention and terms
RFIs and submittals	RFIs per unit of contract value, share with cost impact, response times
Change events, PCOs, change orders	Cause, rate versus contract, time from RFI to approval, proximity to DoA limits
Claims and notices	Frequency, clauses cited, outcomes
Progress invoices and payments	Approval days, cut percentage, release days, percent complete versus inspections
Inspections, NCRs, punch lists	Rejection rates, re-inspections, closure times by contractor
Workflow history	Approver, delegate, step durations, returns, overrides
Daily reports, timesheets, schedule updates	Manpower versus progress claimed, schedule progress versus invoiced progress

Completed projects matter as much as live ones. Capturing the key transactions of finished projects, as Part 6 described for forensic audits, gives the models history to learn from.

AI on a Document Platform Is Not AI on a PMIS

The same false assurance is now appearing with AI. Document platforms and CDEs are adding AI features: summarising documents, drafting correspondence, searching across files, reading scanned forms. These are useful features for a document repository. They are not fraud detection. An AI that reads a change order PDF can summarise what the letter says. It cannot tell whether the rate is the contract rate, whether the approver was within their authority, or whether the same contractor's invoices are approved twice as slowly as everyone else's, because none of that is held as data in the repository.

Question an integrity reviewer asks	AI on a document platform	AI on PMWEB data
Which change orders were priced above contract rates?	Can find letters mentioning rates; cannot compare them	Compares change order line items with the schedule of values
Which approvals exceeded the approver's DoA?	Sees who stamped a file	Tests approved value against the DoA rule for that role
Which contractor's invoices are cut the most?	Cannot see submitted versus approved amounts	Calculates cut percentage for every invoice
Which bids were unbalanced?	Can open the bid file	Ratios every line item against the estimate
Is this pattern new or recurring?	No history of structured outcomes	Learns from dispositions recorded on red flags

An AI answer that sounds confident but rests on unstructured documents is the most persuasive form of false assurance yet. The safeguard is the same as for every other tool in this series: put the transactions in a PMIS first, then apply AI to data that can be tested.

Reading PMWEB and the ERP Together

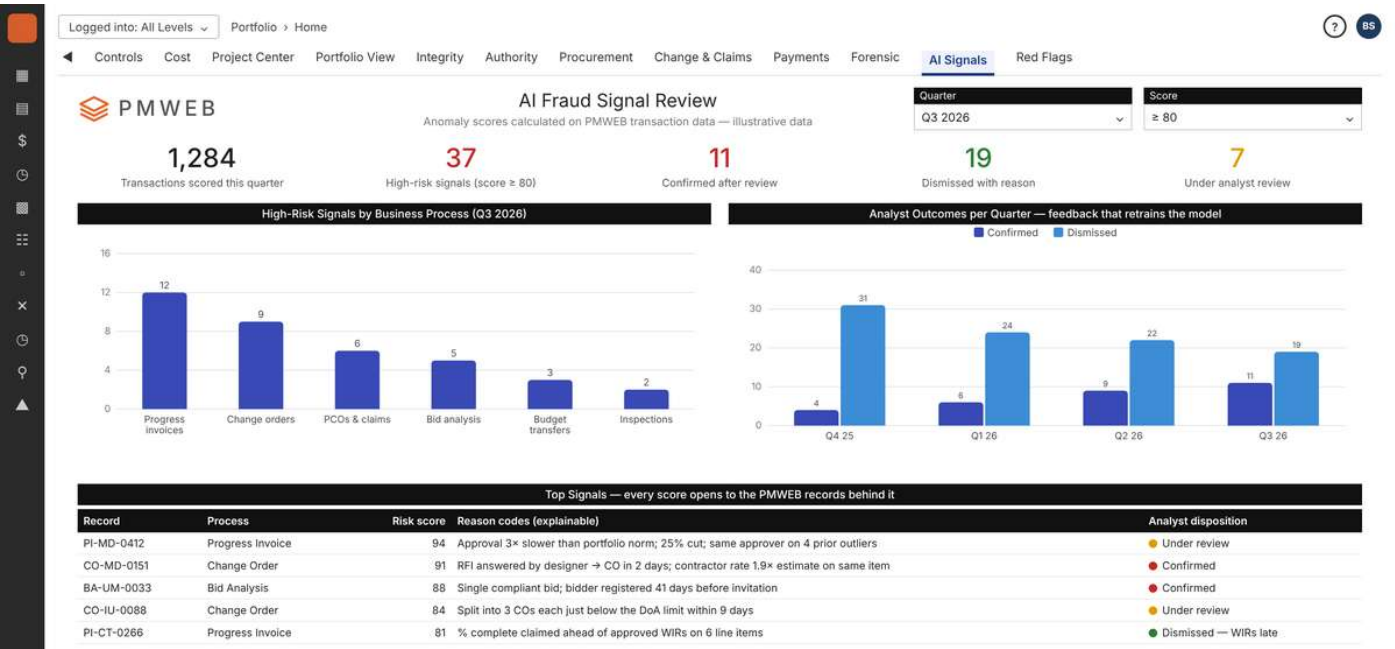
Some fraud only shows when project data and finance data are compared: a payment in the ERP with no approved certificate in PMWEB, a vendor bank detail changed shortly before a large payment, or an invoice paid twice through different channels. askAIRO, a CMCS offering for PMWEB clients, is an AI assistant built on the Model Context Protocol (MCP) that answers questions from PMWEB and the client's ERP together. It works with PMWEB hosted on-premises or in the cloud and with the large language model of the client's choice, including one the client hosts on its own servers, which keeps sensitive investigation data inside the organisation.

No excuse to stay on the wrong platform

If your project information sits on a platform that cannot hold transactions as data, no AI added to it will detect fraud reliably. **Migrating to a PMIS like PMWEB is the prerequisite for AI-assisted fraud detection**, not an alternative to it.

From Scores to Decisions

A risk score is useful only if a reviewer can see why it was given and what to do next. The AI signal review below shows how this looks in practice.



AI Fraud Signal Review — anomaly scores calculated on PMWEB transaction data and presented as a Power BI report embedded in PMWEB. Illustrative data.

Each high-risk signal carries reason codes in plain language, for example an invoice approved three times slower than the norm with a 25% cut, by an approver who appears on four earlier outliers, or a change order split into three just below the DoA limit within nine days. Each opens to the PMWEB records behind it. Each is reviewed by an analyst and closed with a disposition. The quarterly chart shows the effect of that feedback: as confirmed and dismissed outcomes retrain the model, dismissed signals fall and confirmed ones rise, which means reviewers spend more of their time on real issues.

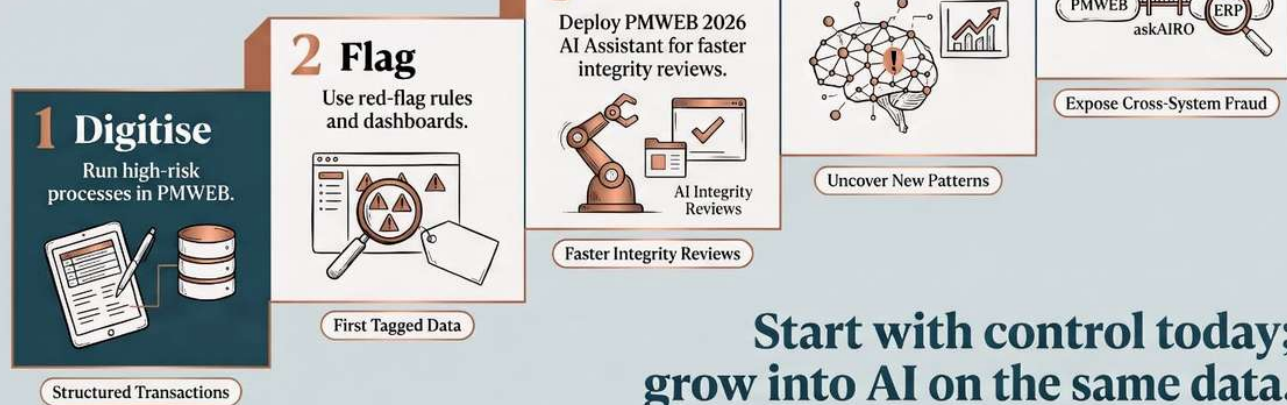
Using AI for Fraud Detection Responsibly

- **A score is a question, not an accusation.** Signals start reviews; investigations and due process decide outcomes.
- **Explainability is mandatory.** Every score must show the features and records that drove it, or it cannot be acted on fairly.
- **Humans decide, and their decisions are recorded.** Dispositions are captured on the red-flag record and become training data.
- **Security follows PMWEB.** AI tools see only what the user's role allows; investigation records are restricted.
- **Data stays governed.** Choose deployment and model options that keep sensitive data within the organisation's control.
- **Measure the model.** Track precision (share of signals confirmed), coverage and time to review, and retrain on a schedule.

A Practical Adoption Path

Stage	What the owner does	Outcome
1. Digitise	Run the high-risk processes from Parts 1 to 5 in PMWEB with templates, workflows and DoA rules	Structured, approved, linked transactions
2. Flag	Configure red-flag rules and dashboards; record each flag and its disposition in PMWEB	Exceptions reviewed every period; first tagged data
3. Assist	Use the PMWEB 2026 AI Assistant for find, open, create and help in integrity reviews	Faster reviews within existing security
4. Learn	Add unsupervised anomaly detection, then supervised scoring as dispositions accumulate	Signals on patterns no rule describes
5. Connect	Bring ERP and other sources into the analysis, for example through askAIRO	Cross-system fraud visible

From Digitised Processes to AI-Assisted Fraud Detection



Digitise. Flag. Assist. Learn. Connect.

CMCS | PMWEB Authorised Implementation Partner – GCC & MENA

Gemini Notebook

The Business Case, Restated

Part 1 showed that when fraud risk is priced in, a PMIS repays its cost many times over: avoiding even a quarter of one percent of leakage on a large capital portfolio is worth more each year than the system costs to own. AI raises that return further, because the same data that enforces controls now also finds the patterns that rules miss, and every reviewed signal makes the next one more accurate. The investment that prevents fraud is the same investment that makes AI possible.

The funder's lens — ministries of finance and sovereign funds

- Ministries and funds that see many entities hold the largest potential data set for fraud analytics, provided those entities capture transactions in a consistent, structured way.
- Requiring a common PMIS standard across funded entities is what makes portfolio-wide AI signals possible.

Adviser's checklist — for consultants recommending project governance

Questions to ask in the diagnostic

- Is the client being offered AI on a document platform as a fraud-detection answer?
- Does the client hold enough structured, approved transaction history for analytics to learn from?
- Are red-flag dispositions recorded so they can become training data?

Recommendations to put in the governance report

- Sequence AI after structured capture: digitise, flag, assist, learn, connect.
- Require explainable reason codes and human disposition for every AI signal.
- Keep sensitive investigation data within the client's control when selecting AI deployment options.

Series Summary

Part	Fraud risk addressed	Core PMWEB control
1	Governance gaps and data silos	Procedures executed as templates, workflows and one cost ledger
2	Unauthorised or unaccountable approvals	DoA embedded in workflow, formal delegation, complete output forms
3	Procurement fraud and unbalanced bids	Prequalification gates and line-item bid analysis against the estimate
4	Over-priced changes, design errors, claim strategies	Linked RFI, change event, PCO, change order and claim records
5	Abuse of approval power on payments	Invoice checklist, workflow history and abnormalities reporting
6	Losses already incurred	Forensic rebuild of the record and cross-project correlation
7	Patterns no rule describes	PMWEB 2026 AI Assistant and learning analytics on PMWEB data

Key takeaway

AI does not replace fraud controls. It depends on them. Every template, workflow, link and disposition captured in PMWEB is a data point that makes detection more accurate.

AI on a document repository summarises what was written; AI on PMWEB tests what was approved.

Owners who digitise their processes in PMWEB today get control now, AI-assisted review with PMWEB 2026, and the data foundation for learning analytics as their transaction history grows.

Migration to a PMIS is the prerequisite for AI fraud detection, not an alternative to it.

Series complete: Parts 1 to 7 are available on LinkedIn and on the CMCS website. Owners who want to start can begin with the high-risk processes in Parts 2 to 5 on a new programme, and extend from there.

Talk to us: If your projects run on Aconex or another document management system, a CDE without DoA-driven workflows, a PMIS without ERP integration or full cost and contract management, or no system at all, there is no longer an excuse to stay: migrate your fraud-exposed processes to a PMIS like PMWEB. CMCS can assess your current platforms and data, start PMWEB on a new programme, integrate it with your ERP and document platforms, and migrate legacy project data, including from Oracle Aconex and Oracle Unifier. To see this, including PMWEB 2026 AI and red-flag dashboards, contact CMCS at info@CMCS-MENA.com. Management consultants designing project governance for their clients are welcome to use these frameworks; CMCS works alongside consulting firms to turn governance recommendations into configured PMWEB processes. Ministries of finance and sovereign funds can also see how a common PMWEB standard across funded entities gives them verified, portfolio-wide visibility.

#PMWEB #CMCS #PMWEB2026 #AI #FraudDetection #MachineLearning #askAIRO #CapitalProjects #PMIS #Integrity #CDE #DocumentManagement #ERPIntegration #ManagementConsulting #ProjectGovernance #MinistryOfFinance #SovereignWealthFund

About the Author

Bassam Samman, PMP, PSP, EVP, GPM is the Chairman and Chief Executive Officer of CMCS FZCO, the PMWEB Authorised Implementation Partner for the Gulf Cooperation Council and broader Middle East and North Africa region. CMCS holds the PMWEB Global Partner of the Year 2025 designation and serves capital project owners, contractors and consultants across the UAE, Saudi Arabia, Qatar and Kuwait.

Bassam has over four decades of experience providing project management, project controls services and project management information systems to more than two hundred capital projects with a combined value exceeding one hundred billion US dollars. He is the author of four published books on project management digitalisation, and has lectured at more than three hundred and fifty international events. He is a co-founder of the Project Management

Institute Arabian Gulf Chapter. He holds a Master's degree in Engineering Administration (Construction Management), with Faculty Commendation, from George Washington University and a Bachelor's degree in Civil Engineering from Kuwait University, with executive education at Harvard Business School and London Business School.

About PMWEB

PMWEB is an enterprise-class, web-based capital construction project management platform trusted by organisations worldwide including Harvard University, the United Nations, and Atlanta Airport. Built on Microsoft .NET technology, PMWEB manages the entire project lifecycle within a single integrated platform — from portfolio planning and cost management through document control, procurement, scheduling, asset management, and business intelligence. With 150+ pre-configured SSRS reports, drag-and-drop dashboard design, multi-currency support, and open REST/SOAP API integration, PMWEB delivers enterprise capability with implementation timelines measured in months, not years.

About CMCS

CMCS (Collaboration, Management and Control Solutions) is the PMWEB Authorised Implementation Partner for the GCC and MENA regions and PMWEB Global Partner of the Year 2025, with offices in Dubai, Abu Dhabi and Riyadh. CMCS specialises in digital project management solutions for real estate developers, government entities, infrastructure owners, project management consultants and construction companies across the Middle East and North Africa.