navro

PAYROLL SECURITY

The Payroll Security Audit checklist

23 critical questions to identify CSV and bank file vulnerabilities before your Compliance Team does.

6	23	4
Risk Domains	Questions	Risk Levels

Based on SOC 2, ISO 27001 & GDPR compliance frameworks

navro.com

23 Payroll security questions your auditors will ask about CSV files

Your company just signed a major enterprise client who requires SOC 2 Type II certification. During the readiness assessment, the auditor asks: Who can access the payroll CSV files between export from your HRIS and upload to the bank? Where are those files stored? How do you verify no one modified payment amounts? Can you show me the complete audit trail for last month's payroll run?

For most payroll teams relying on CSV workflows, these questions expose uncomfortable gaps.

File-based payroll workflows, exporting CSVs from HRIS, manipulating them in Excel, uploading to bank portals, are universal in the industry. But what's "normal" isn't necessarily compliant. Most payroll teams have never subjected their CSV workflows to formal security assessment using the same criteria external auditors apply.

The result is hidden vulnerabilities that only surface during high-stakes audits or, worse, after a data breach or payment fraud incident. This payroll security audit checklist translates the questions SOC 2, ISO 27001, and GDPR auditors actually ask about payment workflows into a practical self-assessment tool. Walk through 23 critical questions across six risk domains, score your current workflows against compliance requirements, and identify exactly where CSV and Excel dependencies create audit exposure before your compliance team or external regulators do the same assessment with higher stakes.

The checklist covers Access Control and Authentication, Data Integrity and Validation, Audit Trail and Traceability, Segregation of Duties, Encryption and Data Protection, and Exception Handling, with scoring guidance and specific remediation actions for each gap identified. Plus: how API-led payroll infrastructure systematically addresses every checklist item through built-in controls rather than compensating manual processes.

How to use this Payroll Security Audit checklist

This checklist is organised around six risk domains that auditors examine in payment workflows, based on SOC 2 Trust Services Criteria and ISO 27001 Annex A controls (specifically A.9 access control, A.12 operations security, and A.18 compliance).

The question format matters. Every question asks: **Can you demonstrate, prove, or show evidence of this control?**
Not: **Do you have a policy about it?**

Auditors require verifiable evidence, not documented intentions.

Scoring Method

For each question, record one of three answers.
Then calculate domain scores. “No” answers in Access Control or Segregation of Duties typically represent Critical risk, meaning likely audit findings and potential compliance violations. Gaps in Audit Trail and Encryption are High risk, creating regulatory exposure. Validation and Exception Handling gaps are Medium risk, with direct operational and reputational consequences.

- YES
  Control exists with documented, retrievable evidence
- PARTIAL
  Control exists but lacks consistent documentation or systematic enforcement
- NO
  Control is missing entirely — a direct audit finding

CRITICAL RISK

01. Access Control & Authentication

1

Can you list every person who accessed payroll CSV files in the past 90 days, with timestamps?

This tests whether file access is logged at all. Files stored on individual desktops or Downloads folders generate no access log. If you cannot produce this list on demand, you have no access control evidence.

☐ Yes ☐ Partial ☐ No

2

Are payroll file permissions managed through centralised identity management (SSO/Active Directory), or does access depend on whoever has the file or login credentials?

This exposes informal access sharing. Bank portal passwords shared via Slack or email are a red flag that appears in nearly every payment-related audit finding.

☐ Yes ☐ Partial ☐ No

3

How do you revoke access to payroll files when an employee leaves or changes roles, and can you prove files stored on local machines were deleted?

Offboarding controls for file-based workflows are almost always incomplete. Former employees' laptops potentially still containing payment files represent an ongoing data breach risk under GDPR Article 5.

☐ Yes ☐ Partial ☐ No

4

Does your bank portal login use multi-factor authentication, and is that login shared among multiple team members?

Shared credentials eliminate individual accountability and make attribution of unauthorised activity impossible during a forensic investigation.

☐ Yes ☐ Partial ☐ No

MEDIUM RISK

02. Data Integrity & Validation

5

When payroll exports CSV from HRIS and manually adds columns or reformats data for bank upload, how do you verify amounts weren't accidentally changed?

Reliance on "eyeballing" totals is not a control. Auditors will ask for checksum or hash verification evidence. Integrity failures are often invisible until employees report missing salary.

☐ Yes ☐ Partial ☐ No

6

Do you validate bank account details (sort codes, account numbers, IBAN formatting) before submitting payment files, or does validation happen after upload when banks reject files?

Post-facto validation, discovering errors only after bank rejection, is a systemic gap in CSV payroll compliance checklists that auditors treat as a process maturity failure.

☐ Yes ☐ Partial ☐ No

7

Can you detect if a payment amount or recipient was altered between CSV export and final bank upload, and would you notice within minutes or days?

If the honest answer is "Days, when employees report missing payments," you have a tampering detection gap that directly affects GDPR Article 32 obligations around data integrity.

☐ Yes ☐ Partial ☐ No

8

How do you reconcile the original HRIS payroll report against the final bank file to confirm no payments were added, removed, or modified?

The absence of systematic reconciliation is one of the most common CSV security risks in payroll. Manual total comparisons miss row-level changes.

☐ Yes ☐ Partial ☐ No

HIGH RISK

03. Audit Trail & Traceability

9 → 10 → 11 → 12

For any payment in last month's payroll, can you produce a complete chain of custody showing who exported, who modified, who reviewed, and who uploaded the file containing that payment?

This is the end-to-end traceability question. If any step in that chain relies on email evidence or memory, it will not satisfy SOC 2 auditors or ISO 27001 reviewers.

☐ Yes ☐ Partial ☐ No

Where is the evidence stored that proves Maker Checker review happened before upload, and is that evidence tamper proof?

"We email files for approval but those emails aren't systematically saved" is a direct audit failure. Email chains are not tamper proof audit trails.

☐ Yes ☐ Partial ☐ No

Can you retrieve the exact version of the payment file that was uploaded to the bank, versus just the original HRIS export?

File versioning that relies on desktop filenames like "Payroll_FINAL_v3_ACTUAL.xlsx" is not version control. It is not retrievable evidence under scrutiny.

☐ Yes ☐ Partial ☐ No

How long do you retain payroll file audit trails, and do they meet your statutory retention requirements, typically six to seven years?

Most CSV security risk assessments for payroll skip retention entirely. Auditors do not.

☐ Yes ☐ Partial ☐ No

CRITICAL RISK

04. Segregation of Duties (SOD)

13

Can the same person who prepares the payroll CSV also upload it to the bank and approve the payment batch, and does your system enforce separation?

If there is no technical control preventing a single person from preparing and executing a payment, SoD is a policy, not a control. Policies alone do not satisfy SOC 2 auditors.

☐ Yes ☐ Partial ☐ No

14

How do you ensure the person with bank portal upload access cannot also modify payment amounts in the CSV before upload?

This identifies combined prepare and execute risk. In small payroll teams where one person "does everything," this represents an inherent fraud risk that no compensating control fully mitigates.

☐ Yes ☐ Partial ☐ No

15

Is payroll review and approval documented through a separate system with access controls, or does it rely on someone else looking at the file before upload?

Informal approval is not approval evidence. Auditors require system-enforced review steps with timestamped records.

☐ Yes ☐ Partial ☐ No

16

Can you demonstrate that no single individual has end-to-end control over payroll from HRIS export through bank upload confirmation?

This tests your overall SoD architecture. If you cannot demonstrate this with system evidence, you have a Critical-level payroll file security assessment gap.

☐ Yes ☐ Partial ☐ No

HIGH RISK

05. Encryption & Data Protection

17

Are payroll CSV files encrypted at rest (on desktops, shared drives, and email) and in transit during upload to bank portals?

Unencrypted files on laptops are not an edge case. They are the default state in most file-based payroll workflows and represent direct exposure under GDPR Article 32 technical measures requirements.

☐ Yes ☐ Partial ☐ No

18

When payroll files are emailed for review or sent to local payroll partners and accountants, are those emails encrypted and do they expire or revoke access?

Payment files sent as plain email attachments are a GDPR violation waiting for a regulator's attention. The ICO has issued enforcement action for exactly this type of inadequate technical measure.

☐ Yes ☐ Partial ☐ No

19

Can you list every location, including laptops, desktops, shared drives, email inboxes, and USB drives, where copies of payment files might exist, and confirm all are encrypted?

File sprawl is the encryption problem no policy solves. Each additional copy is an additional exposure point.

☐ Yes ☐ Partial ☐ No

20

Do your CSV files containing employee bank details and salaries meet GDPR Article 32 requirements for appropriate technical measures to protect personal data?

"Appropriate technical measures" is not aspirational language. It is a legal obligation. Unencrypted or loosely controlled payment files containing salary and bank account data will not satisfy an ICO investigation.

☐ Yes ☐ Partial ☐ No

MEDIUM RISK

06. Exception Handling & Payment Status

21 → 22 → 23

When a bank rejects a payment from your uploaded CSV, how quickly do you know, and does your team monitor for rejections in real time?

Discovering payment failures only when employees ask where their salary is represents a critical visibility gap. It also means your statutory and tax payment obligations face the same undetected rejection risk.

☐ Yes ☐ Partial ☐ No

Can you prove to an employee or auditor that a specific payment was successfully received by their bank, with a timestamp and reference number?

Proof of payment on demand is an audit requirement and an employee relations obligation. If you cannot produce it within minutes, your payment status infrastructure is inadequate.

☐ Yes ☐ Partial ☐ No

How do you track and resolve payment exceptions, including rejections, returns, and late processing, from initial detection through resolution and employee communication?

Manual exception tracking in spreadsheets or email threads fails both the operational and audit trail tests simultaneously.

☐ Yes ☐ Partial ☐ No

Calculate your risk score

Count your “No” and “Partial” answers by domain, then apply these risk thresholds:

Risk Scoring Thresholds

GAP COUNT	RISK LEVEL	REQUIRED ACTION
0–3 gaps	Low	Tactical improvements and documentation updates
4–8 gaps	Medium	Systematic process upgrade required
9–15 gaps	High	Infrastructure change necessary before next audit
16+ gaps	Critical	Immediate remediation required

Domain-Based Risk Weighting

Critical risk	**Access Control & Segregation of Duties** – Likely audit findings and potential compliance violations
High risk	**Audit Trail & Encryption** – Regulatory exposure and limited forensic capability
Medium risk	**Validation & Exception Handling** – Operational impact and reputational damage

The uncomfortable reality

Most payroll teams score between 10 and 18 gaps. CSV workflows inherently lack built-in controls. Compensating controls, meaning policies and manual checks, exist but lack systematic enforcement or retrievable evidence. That’s not a people problem. It’s an architecture problem.

Sample interpretation: If you answered “No” to **Q1, Q5, Q9**, and **Q21,** you have critical gaps in access logging, integrity verification, audit trail, and payment status visibility. These four answers alone would trigger audit findings in a SOC 2 or ISO 27001 review.

Scoring summary

Complete this summary after working through all six domains. Use it to brief compliance and finance leadership on your current payroll security posture.

DOMAIN	RISK LEVEL	YES	PARTIAL	NO	PRIORITY ACTION
01. Access Control & Authentication	Critical				
02. Data Integrity & Validation	Medium				
03. Audit Trail & Traceability	High				
04. Segregation of Duties	Critical				
05. Encryption & Data Protection	High				
06. Exception Handling & Payment Status	Medium				
TOTAL					

Three remediation pathways based on your score

0–3 Gaps: Tactical Fixes

Implement file encryption, centralise file storage with access logging, document SoD in policy, and add manual reconciliation checkpoints. These measures buy time but do not eliminate the inherent vulnerabilities in file-based architecture. Auditors will accept them as interim controls with documented remediation plans.

4–15 Gaps: Process Upgrade

Automate file transfer via SFTP with audit logging, implement a workflow management system for maker-checker enforcement, and add pre-upload validation scripts. This reduces manual risk but still relies on file architecture as the foundation, meaning each gap you close creates a new compensating control to maintain.

16+ Gaps: Infrastructure Evolution

Migrate to API-led payroll infrastructure that builds controls into the system rather than compensating around files. This is the systematic solution. API authentication addresses Access Control questions directly. Immutable API logs address Audit Trail. Role-based workflow enforcement addresses SoD. Real-time payment status addresses Exception Handling.

The decision rule is straightforward: if you have five or more Critical or High risk gaps, tactical fixes will not satisfy external auditors. The architecture itself, CSV export to manual manipulation to file upload, is the vulnerability that no amount of policy can fully mitigate. As covered in Navro's article on tackling international payment challenges, the organisations that solve this structurally outperform those that paper over the gaps.

CSV workflow VS. API infrastructure

This table is not a theoretical comparison. Each row corresponds directly to checklist questions where CSV workflows produce “No” or “Partial” answers and API infrastructure produces “Yes” answers by default, because the controls are structural rather than procedural.

CONTROL AREA	CSV WORKFLOW REALITY	API INFRASTRUCTURE REALITY
Access Control	File access unlogged, credentials shared	API keys, role-based access, full auth logs
Data Integrity	Manual reformatting, no hash verification	Pre-run COP/VOP validation built in
Audit Trail	Email approvals, filename versioning	Immutable timestamped logs per transaction
Segregation of Duties	Policy-dependent, technically unenforced	System-enforced workflow with role controls
Encryption	Files at rest on local machines	No file to encrypt; data in transit via TLS
Payment Status	Batch rejection discovered hours later	Real-time status per payment with reference

What auditors accept as evidence

Understanding what constitutes acceptable evidence matters as much as knowing which controls to implement. This is where many payroll teams misjudge their readiness.

CONTROL AREA	ACCEPTED	NOT ACCEPTED
Access Control	System-generated access logs with user IDs, timestamps, and actions	“We restrict who knows the password”
Data Integrity	Automated checksum comparisons or cryptographic hash records	Printed total comparisons or visual review records
Audit Trail	Immutable system logs stored separately from the operational system	Email threads, even if faithfully preserved
Segregation of Duties	Role-based access controls enforced at system level, where the system physically prevents a preparer from also approving	Job descriptions or organisational charts
Encryption	Configuration records showing encryption standards applied at rest and in transit, with key management documentation.	“Our IT team handles that”
Exception Handling	Documented escalation workflows with timestamped records from detection through resolution.	“We check the bank portal every morning”

Building the business case for infrastructure investment

If your assessment revealed a High or Critical score, you may already recognise that tactical fixes are a holding pattern. The harder conversation is usually internal: how do you justify infrastructure investment when the current workflow “hasn’t caused a problem yet”? Three arguments tend to land with finance and executive stakeholders.

Regulatory cost of failure

GDPR enforcement actions for inadequate technical measures have ranged from five-figure fines for small organisations to penalties representing a meaningful percentage of annual turnover for larger ones. A documented failure to implement appropriate technical measures for payroll data, which combines salary information and bank account details, represents exactly the category of exposure the ICO and equivalent regulators pursue.

Audit remediation cost

When external auditors identify material weaknesses, organisations typically face a remediation cycle that includes additional audit fees, accelerated timeline pressure, potential scope limitations on certifications, and internal resource cost. Pre-empting findings through self-assessment and planned remediation is almost always less expensive than reactive remediation under audit pressure.

Operational risk made concrete

The scenarios are not hypothetical. Payment file tampering, whether malicious or accidental, results in employees not receiving salaries on time. The reputational and legal consequences of late or incorrect payroll, compounded by an inability to produce audit evidence of what happened, represent the kind of operational risk that finance leadership understands in direct terms.

Frequently asked questions

How often should we run this payroll security assessment?

Run a full assessment annually at minimum, and after any significant change to your payroll workflow, HRIS system, banking relationships, or team structure. If you are pursuing SOC 2 or ISO 27001 certification, run it at the start of your readiness programme and again three months before your audit date.

Do these questions apply if we use a managed payroll bureau?

Partially. If a payroll bureau handles processing, your direct exposure to Questions 5 – 12 may be reduced. However, Questions 1 – 4 (access control over HRIS data you provide), Questions 17 – 20 (encryption of files you send to the bureau), and Questions 21 – 23 (your visibility into payment status) remain fully applicable. Bureau use does not transfer your GDPR data controller obligations.

What if we are a small team and genuine SoD is impossible?

This is a common and legitimate constraint. In small teams, compensating controls become the answer: mandatory dual sign off via a separate approval system, enhanced monitoring and reconciliation, and documented acknowledgement of the inherent risk with senior sign off. Auditors understand operational reality. What they require is that you have assessed the risk, documented it honestly, and implemented the strongest compensating controls your structure permits. Undocumented SoD gaps with no compensating controls are findings. Documented SoD limitations with robust compensating controls are accepted risks.

Can we build some of these controls using existing tools?

Yes, to a degree. Centralised file storage with access logging (SharePoint or Google Workspace with audit logging enabled), SFTP for file transfer, and workflow tools for approval tracking can address several gaps without infrastructure replacement. The limitation is that these remain compensating controls layered over a file-based architecture. They reduce risk but do not eliminate the fundamental vulnerabilities inherent to CSV based payment workflows.

Conclusion

This 23-question checklist exposes what most payroll teams already suspect: CSV and Excel workflows that “everyone uses” create systematic security, compliance, and operational vulnerabilities that cannot be fully closed with policies and manual controls alone.

If your assessment revealed **8 or more gaps**, particularly in Access Control, Audit Trail, or Segregation of Duties, the workflow itself is the problem, not the people executing it. The useful outcome of this exercise is that you now have objective evidence of the gaps, prioritised remediation actions, and a framework for building the business case for API-led payroll infrastructure that eliminates file-based vulnerabilities by design. Entering an audit with documented self-assessment and a remediation roadmap is a fundamentally different position than discovering gaps under external scrutiny.

Take the scoring summary on page 11 to compliance and finance leadership and agree where to start. Then see how Navro’s API-first global payroll platform closes every checklist item through built-in validation, role-based access controls, immutable audit trails and real-time payment status.

