NovaPay – Document 13: Assessment Summary (Scores, Gaps, Risks)

Version: Content-Only | Generated: 20 Oct 2025 | Company: NovaPay (UK)

EXPECTED OVERALL RISK SCORE (0–100, 100=Excellent)
Overall Score: 65/100 (Medium Risk)

Section Scores
1 Geographic Risk: 62/100 (outdated assessments, manual tracking)
2 Governance: 72/100 (sound structure; reporting cadence gaps)
3 EWRA: 67/100 (annual only; weak scenarios/stress tests)
4 CDD: 67/100 (UBO gaps; backlog; manual share)
5 Adverse Media: 57/100 (periodic, not continuous; backlog)
6 Sanctions: 77/100 (strong coverage; alert fatigue)
7 Transaction Monitoring: 62/100 (tuning delays; backlog)
8 Fraud: 72/100 (good tools; limited AML integration)
9 Technology: 67/100 (data silos; legacy components)
10 Training: 62/100 (completion gap; generic content)
11 Monitoring/Audit/QA: 58/100 (audit overdue; open findings)
12 AI Readiness: 45/100 (governance not in place)

TOP COMPLIANCE GAPS (Severity/Priority)
CRITICAL (High/High)

1. Internal AML audit overdue (should be annual)
2. Remediation slippage: two audit findings past due
3. Country risk assessment not refreshed in 12 months (14 months elapsed)
4. TM rule tuning not performed quarterly (6■month delay)
5. UBO periodic review backlog (~200 overdue)

HIGH (High/Med or Med/High)

6. Adverse media screening limited to onboarding/annual (no continuous feed)
7. PEP screening only at onboarding/annual (no continuous monitoring)
8. Limited AI governance; EU AI Act gap
9. Data silos between fraud, AML, and KYC
10. No ML in TM; rules■heavy approach
11. Training completion below target (94% vs 98%)
12. Alert backlogs (TM ~120; adverse media ~50)

MEDIUM (Med/Med)

13. Board gets compliance reporting quarterly (best practice monthly)
14. Generic training not tailored to risk profile
15. Limited screening of indirect UBOs and PEP associates
16. Manual CDD for ~30% of applications
17. No AI/ML training program for staff
18. Fraud and AML teams operate in silos
19. Emerging risks (crypto, DeFi, AI) not fully integrated in EWRA
20. High TM false positives causing analyst fatigue

EXPECTED RISKS (Category, Likelihood, Impact, Risk Level, Mitigation)

1. Regulatory Sanctions Risk – Regulatory, Medium, High, High. Mitigate: complete internal audit in 60 days; close overdue actions in 90 days.

2. TM Ineffectiveness – Operational, Medium, High, High. Mitigate: quarterly tuning, ML triage, hire 2 analysts.
3. EU AI Act Non■Compliance – Regulatory, High, Medium, High. Mitigate: AI governance framework, inventory, bias testing.
4. Sanctions Screening Failure – Regulatory, Low, Critical, High. Mitigate: optimize fuzzy thresholds, contextual filters, training.
5. CDD Gaps – Regulatory, Medium, Medium, Medium. Mitigate: clear UBO backlog; automate registry verification.
6. Reputational Damage – Reputational, Medium, High, High. Mitigate: close high■priority gaps within 6 months; enhance comms.
7. Financial Loss from Fraud – Financial, Medium, Medium, Medium. Mitigate: integrate fraud/AML; unified risk profile.
8. Data Quality/Integration Risk – Operational, High, Medium, High. Mitigate: unified data platform; improve to 99%+ quality.
9. Staff Turnover/Training – Operational, Medium, Medium, Medium. Mitigate: role■specific training; completion tracking; retention plan.
10. Technology Obsolescence – Operational, Medium, Medium, Medium. Mitigate: upgrade/replace TM (budget $0.5–1.0M).