Oracle Cloud ERP
Risk Signals Readiness Checklist

Use this checklist to assess whether your Oracle Cloud ERP monitoring is producing contextual risk signals or just generating more noise.

1. Monitoring Logic

- [ ] Our Oracle Cloud ERP monitoring rules evaluate more than one condition at a time, rather than relying mainly on single thresholds or one-field exceptions.
- [ ] We combine user context, role sensitivity, transaction details, timing, and recent configuration or master-data changes when evaluating potentially risky activity.
- [ ] We can explain, in plain language, why a flagged event was prioritized as risky and what context made it suspicious.

2. Prioritization and Scoring

- [ ] We use Oracle Cloud ERP risk scoring or a comparable ranking method to sort events by likely significance, rather than reviewing a flat exception list in date order.
- [ ] Reviewers receive a short, prioritized queue of suspicious patterns, not hundreds or thousands of undifferentiated alerts.
- [ ] Our teams trust that the highest-ranked alerts are materially more likely to matter than the rest of the population.

3. Business and Security Context

- [ ] Our rules account for whether the user is new, privileged, temporary, previously flagged, or operating outside normal behaviour patterns.
- [ ] Our monitoring distinguishes between routine activity and the same activity performed by someone with broad Accounts Payable, procurement, finance, or security administration access.
- [ ] We can correlate transactional events with nearby supplier bank-detail changes, approval-rule changes, or configuration updates in the same process area.

4. Review Quality

- [ ] Reviewers do not spend most of their time clearing low-value Oracle ERP false positives.
- [ ] We can show that important alerts are consistently investigated, documented, and either closed or escalated.
- [ ] Internal audit or compliance teams can see evidence that monitoring is operating effectively, not just that alerts exist.

5. Continuous Improvement

- [ ] We regularly tune thresholds when rules fire too broadly and create noise.
- [ ] We retire rules that rarely generate useful cases and refine rules that repeatedly surface genuine issues.
- [ ] Investigation outcomes feed back into the monitoring approach, improving Oracle Cloud ERP contextual risk detection over time.

6. Outcomes

- [ ] Our monitoring output helps us find genuinely suspicious events before audit, finance, or the business escalates them.
- [ ] Control owners generally trust the alert population instead of treating it as a large export to be filtered manually.
- [ ] We have seen progress in reducing noise while improving confidence that real issues stand out clearly enough to be investigated.

Results & Next Steps

*Count how many statements you can honestly mark **"Yes"**:*

> **0–5 Yes Answers:** Your Oracle Cloud ERP monitoring is likely still dominated by noise, flat alerts, and low reviewer trust.

> **6–11 Yes Answers:** You have some contextual monitoring elements in place, but gaps in scoring, correlation, or review discipline are still limiting effectiveness.

> **12–18 Yes Answers:** Your monitoring approach is moving toward contextual risk detection, with stronger prioritization and better operating evidence.