ARE YOUR ORACLE ERP CONTROLS FAILING SILENTLY?

9-Question Self-Assessment for Oracle IT and Audit Leaders

> **Target Audience:** Oracle ERP Cloud / EBS Directors, IAM Leads, Platform Owners, Internal Audit, and SOX teams.
> **Instructions:** Answer each question. Score: **Yes = 2, Partially = 1, No = 0**. Sum your total and review the maturity bands at the end.

1. Reliance on Oracle-Native Tools

Q1. Do you rely primarily on Oracle-native tools (Oracle ERP, Oracle RMC, built-in reports) for SoD, access monitoring, and control evidence, without an independent platform validating those outputs?

☐ Yes ☐ Partially ☐ No

Why it matters: If Oracle is both "system under test" and primary evidence source, auditors will question independence and IPE.

---

2. Manual vs Automated SoD and Access Reviews

Q2. Are your Oracle SoD and access reviews still heavily manual (exports, spreadsheets, one-off SQL) rather than being driven by an automated, policy-based platform?

☐ Yes ☐ Partially ☐ No

Why it matters: Manual reviews are slow, error-prone, and hard to repeat consistently quarter after quarter.

---

3. Effective Access vs Role Names

Q3. Do your current reports show who has effective access (including role inheritance, data security policies, composite roles, and external entitlements), not just assigned Oracle role names?

☐ Yes ☐ Partially ☐ No

Why it matters: Auditors care who can actually perform high-risk actions, not just who carries a particular role label.

---

4. Coverage of Connected Apps

Q4. Do you have a single view of SoD, elevated access, and high-risk activity that spans Oracle ERP and key connected systems like ServiceNow, Salesforce, Coupa, Kyriba, and your IdPs?

☐ Yes ☐ Partially ☐ No

Why it matters: High-risk workflows span multiple platforms; a single-system view misses critical context.

---

5. Independence of Control Evidence

Q5. Can your auditors trace critical control evidence (access, SoD, configuration changes, and key transactions) to a source outside the Oracle runtime and configuration you administer?

☐ Yes ☐ Partially ☐ No

Why it matters: For Big-4 and SOX, independence of evidence is as important as the control design itself.

---

6. Continuous Monitoring vs Point-in-Time Snapshots

Q6. Do you continuously monitor Oracle access, SoD conflicts, and high-risk transactions, or do you mainly rely on point-in-time assessments tied to audit and certification cycles?

☐ Mostly continuous ☐ Mixed ☐ Mostly point-in-time

Why it matters: Point-in-time checks miss access drift and configuration changes between testing windows.

---

7. Elevated Access and Temporary Overrides

Q7. Do you have systematic monitoring over elevated and temporary access (e.g., close activities, "fire-fighter" roles, emergency fixes) across Oracle and ticketing systems, not just a record that access was granted?

☐ Yes, monitored centrally ☐ Tracked, but not consistently monitored
☐ Mostly manual / ad-hoc

Why it matters: Audit and SOX teams increasingly expect proof that elevated access is both controlled and watched.

---

8. Proving Risk Did Not Materialize

Q8. When someone has elevated or conflicting access in Oracle, can you prove that risk did not materialize (for example, show that no unauthorized postings or changes occurred during that elevation window)?

☐ Yes ☐ Sometimes ☐ Rarely

Why it matters: It's not enough to document exposure; you need evidence that no misuse occurred in the period.

---

9. Single Evidence Backbone vs Spreadsheet Patchwork

Q9. Do you have a single, independent "evidence backbone" for Oracle access, SoD, and high-risk activity, or are you stitching together exports from Oracle, identity, and SaaS tools in spreadsheets?

☐ Single source ☐ Some consolidation ☐ Mostly manual exports

Why it matters: A fragmented evidence story drives audit fatigue, surprises, and recurring findings.

Total Score: _____ / 18

0–6: High exposure, low independence
Oracle is likely self-validating. Heavily dependent on manual work. Audit findings and rework risk are high.

7–12: Improving, but fragile
Coverage, independence, or continuity are still inconsistent. A complex audit or Big-4 scrutiny could expose gaps.

13–18: Strong, but can you scale it?
You have many elements of an independent, continuous model. Focus on scaling as integrations grow.