Oracle Cloud ERP
Role Design Readiness Checklist

Use this quick checklist to see whether your Oracle Cloud ERP roles are helping you prevent risk structurally—or just generating repeat findings during audits.

1. Role Structure and Design

- ☐ Our production role catalog is built around a small set of standard job-role patterns, not one-off roles for individual people.
- ☐ We have documented business responsibilities for each standard role (for example: "AP Invoice Processor – no payments").
- ☐ We can identify which roles inherently violate our segregation of duties (SoD) rules without weeks of analysis.
- ☐ We know which roles are considered "high-risk" or "privileged," why they are high risk, and which data scopes make the risk material.

2. Design-time SoD and Sensitive-access Controls

- ☐ Every new or changed role is automatically checked against our SoD rules before it's deployed or assigned.
- ☐ We apply sensitive-access and data-scope rules—for example, powerful configuration privileges, security privileges, business units, ledgers, and data access sets—at the role and assignment level.
- ☐ Toxic combinations are blocked or escalated at design time, rather than discovered months later in SoD reports.
- ☐ Our primary SoD controls live in a repeatable framework, not only in spreadsheets.

3. Seeded Roles and Inherited Duties

- ☐ We know which Oracle-predefined "seeded" roles have been copied or customized and what extra capabilities they now include.
- ☐ We can produce a plain-language "bill of materials" for any role, including inherited duty roles, aggregate privileges, function security privileges, data security policies, and data access assignments.
- ☐ Business owners and auditors can understand who can do what without relying on screenshots or code-level analysis.
- ☐ We regularly review and reduce duty-role sprawl so roles don’t accumulate unnecessary capabilities over time.

4. Governance and Approvals

- ☐ Every new role or material role change requires an explicit business owner and documented approval.
- ☐ We have a consistent workflow for role design and changes, including who can request, who can approve, and what must be justified.
- ☐ We can show, for any high-impact role, who approved it, when, and for what reason in the last 12–24 months.
- ☐ Exceptions to standard role patterns are visible and tracked, not buried in ad-hoc changes.

5. Emergency and Temporary Access

- [ ] We use time-bound emergency / break-glass roles for production issues and special situations.
- [ ] Emergency access is granted through a controlled process with clear owner, scope, and expiration.
- [ ] We regularly review emergency-access usage and remove or downgrade access once the incident or project is complete.
- [ ] We can demonstrate to auditors that temporary access does not become permanent by default.

6. Monitoring and Certification

- [ ] High-risk roles and privileged users are subject to more frequent certification than ordinary access (not just once a year).
- [ ] Certifications are based on clear role descriptions and risk levels, not just lists of technical names.
- [ ] We monitor role changes over time and receive alerts for high-risk modifications (for example, new powerful duties added to a standard role).
- [ ] We can show a history of role changes and reviews as evidence of operating effectiveness, not just one-time designs.

7. Outcomes and Audit Experience

- [ ] We've seen a decline in structural SoD conflicts over the past 1–2 audit cycles (not just user-specific exceptions).
- [ ] Reliance on emergency or "workaround" access has decreased, rather than becoming a new normal.
- [ ] Repeat findings related to roles, SoD, and privileged access have reduced or disappeared from audit reports.
- [ ] Audit conversations about access and roles focus on our control design and governance, not only on remediation of exceptions.

How to use this checklist

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

> **0–10 Yes Answers:** Role design is likely a major structural source of risk and repeat findings. Start with a focused role design and SoD framework review.

> **11–18 Yes Answers:** You have some structural elements in place, but gaps in design-time checks, traceability, or emergency access are probably still driving issues.

> **19+ Yes Answers:** Your role design foundations are strong. Priorities shift toward automation, continuous monitoring, and tighter integration with change controls and remediation workflows.

To turn this into a practical next step, pair the checklist with a short discovery session where you walk through your answers and map out the top three structural fixes for your Oracle Cloud ERP roles.