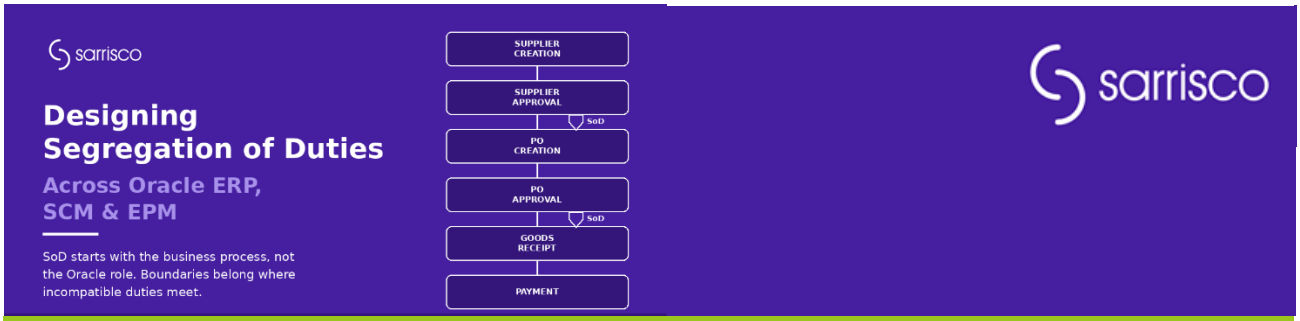


Designing Segregation of Duties Across Oracle ERP, SCM & EPM

Why Segregation of Duties Starts with Your Business, Not Oracle

For many organisations, Segregation of Duties (SoD) is viewed as a compliance exercise.

- A spreadsheet is produced.
- Conflicting Oracle roles are identified.
- Some access is removed.
- The audit requirement is ticked off.

The problem with this approach is that it focuses on **Oracle**, rather than the **business processes Oracle supports**.

At Sarrisco, we believe Segregation of Duties should be designed long before the first Oracle Job Role is assigned.

It should begin by asking a much simpler question:

- **"Which business activities should never be performed by the same individual?"**

Everything else flows from that decision.

Oracle Doesn't Create Segregation of Duties

One of the biggest misconceptions in Oracle Cloud implementations is that SoD is something Oracle delivers.

It isn't.

Oracle provides an incredibly flexible security model capable of enforcing business controls.

But Oracle does not decide what those controls should be.

- Those decisions belong to the business.
- Business leaders determine who owns a process.
- They decide where approvals should occur.
- They define financial authority.
- They identify incompatible responsibilities.

Oracle then provides the security model that enforces those governance decisions.

When organisations reverse that thinking and attempt to design SoD from Oracle Job Roles, the result is often unnecessary complexity, excessive customisation and controls that don't accurately reflect how the business operates.

Think in Business Processes, Not Job Roles

One of the guiding principles within our Oracle Cloud Security Governance & Delivery Framework is simple:

Segregation of Duties should be designed around business processes rather than Oracle privileges.

Take Procure-to-Pay as an example.

The question isn't:

- "Which Oracle role should this user have?"

The question is:

- "Which stages of the Procure-to-Pay lifecycle should this person be responsible for?"

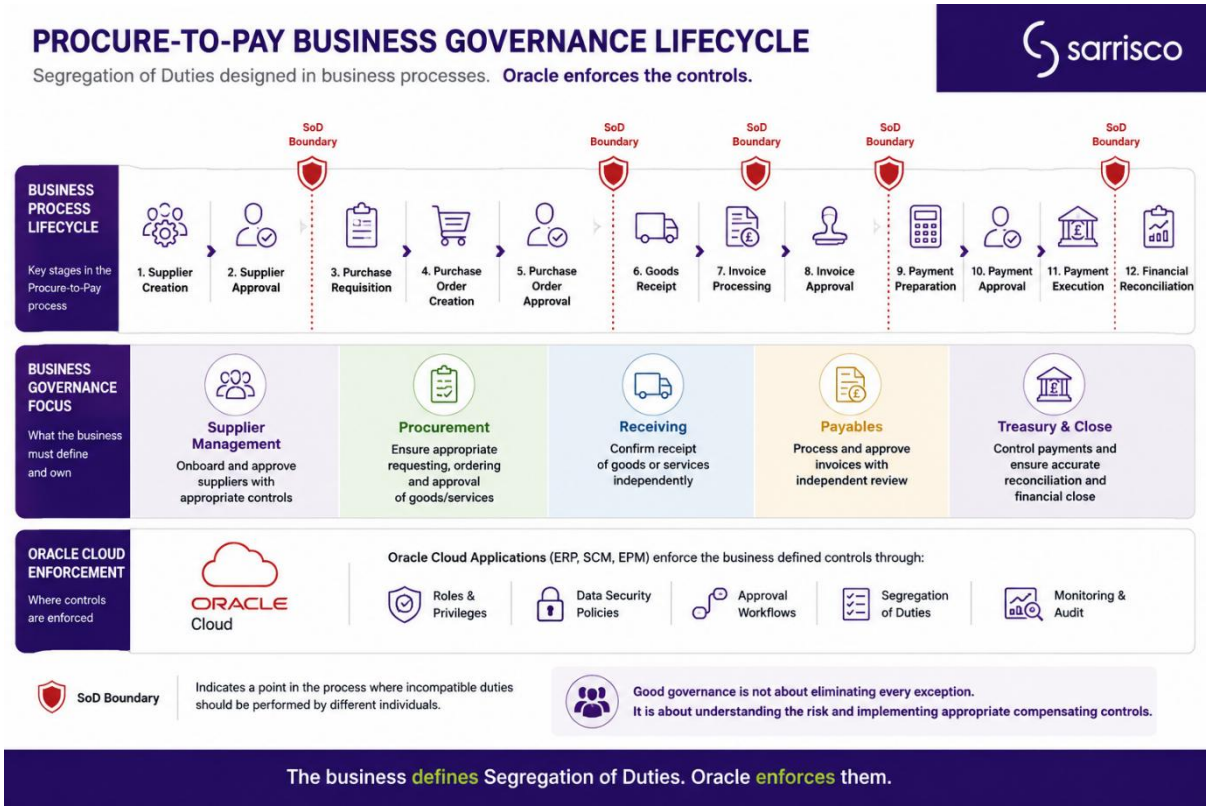
That distinction changes the conversation entirely.

Instead of discussing security configuration, you're discussing operational governance.

A Typical Procure-to-Pay Lifecycle

A mature Procure-to-Pay process naturally separates responsibilities throughout the lifecycle.

Figure 1 illustrates how Segregation of Duties should be designed around business process ownership before Oracle Cloud security controls are applied – Procure-to-Pay Business Governance Lifecycle.



Notice that every Segregation of Duties boundary represents a business governance decision, not an Oracle security decision. Oracle simply enforces the controls that the business has defined

Each stage represents a different business control.

No single individual should normally control multiple incompatible stages without formal approval or compensating controls.

The objective isn't to make processes more complicated.

It's to reduce fraud risk, improve accountability and strengthen financial governance.

Extending the Same Thinking into Oracle EPM

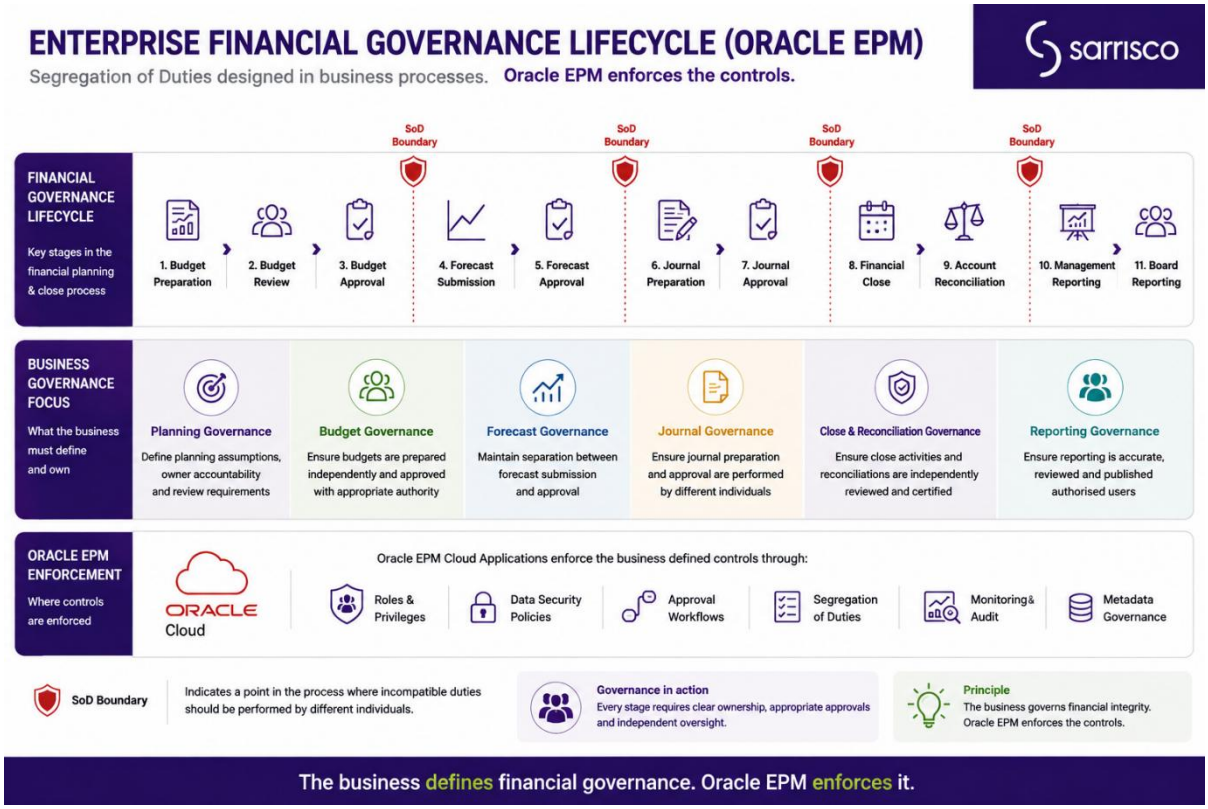
One of the biggest enhancements we've made to our Security Governance Framework is extending these principles into Oracle Enterprise Performance Management (EPM).

Historically, many organisations have focused SoD almost exclusively on ERP.

Yet EPM manages some of the organisation's most sensitive financial information.

- Budgets.
- Forecasts.
- Financial close.
- Enterprise metadata.
- Reconciliations.

Figure 2 illustrates how Segregation of Duties should be designed around business process ownership before Oracle Cloud security controls are applied – Enterprise Financial Governance Lifecycle (Oracle EPM).



If appropriate governance isn't applied, organisations can unintentionally allow individuals to prepare, approve and publish financial information without independent oversight.

The same governance principles therefore apply.

- Budget preparation should remain separate from budget approval.
- Forecast changes should follow controlled approval workflows.
- Journal preparation should remain independent from journal approval.
- Metadata changes should require governance before deployment.
- Financial reconciliations should include independent certification.

The applications may differ.

The governance principles do not.

Figure 2 demonstrates that the same governance principles apply throughout the financial planning and close process. Oracle EPM provides the mechanisms to enforce those controls, but the segregation decisions remain business-owned.

Oracle ERP, SCM & EPM Should Operate Under a Single Enterprise Security Governance Model

As Oracle Cloud estates continue to grow, organisations increasingly operate multiple Oracle Cloud applications.

- Finance.
- Procurement.
- Supply Chain.
- Planning.
- Financial Close.
- Enterprise Data Management.

Unfortunately, many organisations continue to design security independently within each application.

- Different teams.
- Different standards.
- Different approval models.
- Different approaches to governance.

The result is inconsistency.

Instead, organisations should establish a single enterprise security framework that defines common principles across Oracle ERP, SCM and EPM.

That means consistent approaches to:

- Business responsibilities
- Role ownership
- Segregation of Duties
- Least Privilege
- User provisioning
- Approval governance
- Operational security
- Quarterly access reviews

The applications may evolve independently.

The governance model should not.

A single governance model provides consistency of policy, accountability and control across the Oracle Cloud estate, regardless of how many applications are introduced over time.

Designing for Exceptions Rather Than Perfection

Every organisation is different.

Smaller organisations cannot always separate every activity.

Operational realities sometimes require individuals to perform multiple responsibilities.

That doesn't mean governance has failed.

It means governance must become risk-based.

Where full segregation isn't practical, organisations should formally assess the risk, obtain business approval and introduce compensating controls.

Examples include:

- Independent management review
- Exception reporting
- Increased audit activity
- Enhanced approval workflows
- Regular access certification

Good governance isn't about eliminating every exception.

It's about ensuring every exception is understood, documented and appropriately controlled.

Segregation of Duties Doesn't End at Go-Live

One of the biggest mistakes organisations make is treating SoD as an implementation deliverable.

In reality, it is an operational discipline.

- Organisations evolve.
- People change roles.
- Departments restructure.
- New Oracle functionality is introduced every quarter.

Without ongoing governance, today's compliant security model can quickly become tomorrow's audit finding.

- Regular access reviews.
- Quarterly SoD assessments.
- Privilege reviews.
- Dormant account monitoring.
- Emergency access governance.

These activities should become part of normal business operations, not just implementation activities.

Final Thoughts

Segregation of Duties has never been about Oracle roles.

It has always been about protecting the integrity of business processes.

Oracle simply provides the technology to implement those decisions.

When organisations design SoD around business responsibilities rather than application configuration, they create controls that are easier to understand, easier to maintain and significantly more effective at reducing operational risk.

That's why, at Sarrisco, we design Segregation of Duties before we design security.

Because strong governance doesn't begin with technology.

It begins with understanding how your business should operate.

Our Security Governance & Delivery Framework is currently being applied on one of the UK's largest Oracle Cloud transformation programmes currently underway, where security is delivered as a dedicated workstream spanning ERP, SCM, EPM and Oracle Identity & Access Management (IAM).

At Sarrisco, we help organisations design Oracle Cloud Security around business governance, not application configuration. Because secure ERP isn't created by assigning roles, it is created by designing the right business controls from the outset.

This article forms part of the Sarrisco Oracle Cloud Security Governance & Delivery Framework series.

Contact us to learn how Oracle Cloud Security Governance & Delivery Framework can support your long-term Oracle Cloud success.

.

connect with us

info@sarrisco.com

www.sarrisco.com

ORACLE | Partner

The power behind our modern delivery method of cloud solutions