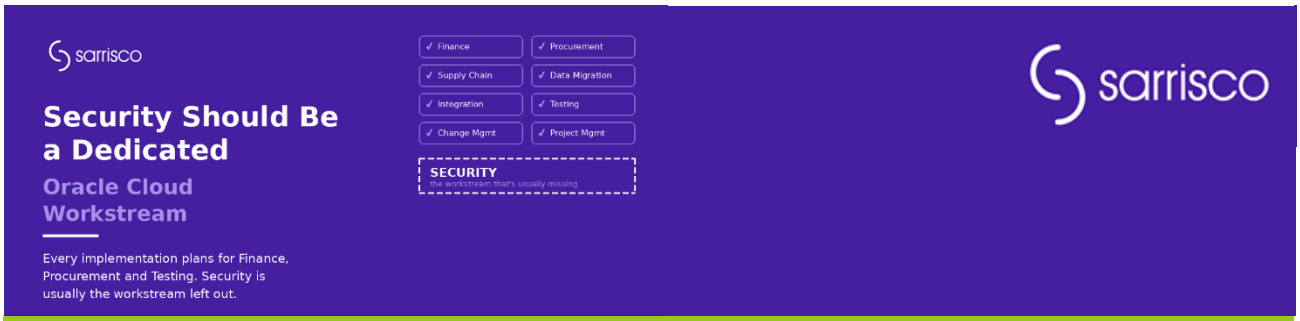

Why Security Should Be a Dedicated Oracle Cloud Workstream

Treating Security as a Technical Task Is One of the Biggest Risks in an Oracle Cloud Programme

Every Oracle Cloud implementation begins with a familiar set of workstreams.

- Finance.
- Procurement.
- Supply Chain.
- Data Migration.
- Integration.
- Testing.
- Change Management.
- Project Management.

Each has defined deliverables, governance, workshops and dedicated resources.

Yet one workstream is often missing.

- Security.

Instead of being recognised as a business-critical discipline, security is frequently treated as a technical activity that can be completed towards the end of the implementation.

- Roles are configured.
- Users are provisioned.
- Testing is completed.
- The project goes live.

By then, many of the most important security decisions have already been made, without a structured governance framework to support them.

Security Touches Every Phase of an Oracle Implementation

Security isn't a single deliverable.

It influences almost every aspect of an Oracle Cloud programme.

During solution design, security defines how business responsibilities are translated into roles and access models.

During business process design, it identifies where independent approvals are required and where Segregation of Duties (SoD) controls should exist.

During integration design, it determines how users will be authenticated and provisioned through Oracle Identity and Access Management (IAM) and enterprise identity platforms such as Microsoft Entra ID.

During testing, it validates not only functional processes but also role assignments, data security, workflow approvals and audit controls.

Even after go-live, security continues to evolve through access reviews, Oracle quarterly updates, role optimisation and operational governance.

Security isn't something that appears during the final stages of a project.

It is present from discovery through to business-as-usual operations.

Security Is Business Governance, Not Technical Configuration

One of the biggest misconceptions in Oracle Cloud programmes is that security is primarily about configuring Job Roles.

In reality, the technical configuration is one of the final steps.

The real work begins much earlier.

The business must first answer questions such as:

- Who owns each business process?
- Which responsibilities require independent approval?
- Which activities should never be performed by the same individual?
- What level of authority is appropriate for different roles?
- Which organisational data should each user be able to access?

These are governance decisions.

Oracle simply provides the security model that enforces them.

Without business ownership, technical security becomes inconsistent, difficult to maintain and increasingly expensive to change.

The Cost of Leaving Security Too Late

We've seen many programmes where security becomes a reactive exercise.

Business process design is complete.

Approval hierarchies are already agreed.

Integration has been developed.

Testing has begun.

Only then is a Security Lead asked to create the roles.

By that stage, fundamental governance decisions have already been embedded into the solution.

Changing them often affects:

- Business processes
- Workflow approvals
- Reporting
- Testing
- Training
- Cutover planning

Late security decisions rarely remain isolated.

They create ripple effects across the entire programme.

The earlier security is introduced, the lower the implementation risk.

One Framework Across ERP, SCM and EPM

Modern Oracle Cloud programmes rarely implement a single application.

Many organisations now deploy Oracle Fusion ERP, Supply Chain Management (SCM), Enterprise Performance Management (EPM) and Oracle Identity and Access Management (IAM) as part of a connected enterprise platform.

Treating security independently within each application creates unnecessary inconsistency.

- Different role design standards.
- Different approval models.
- Different approaches to Segregation of Duties.
- Different governance processes.

Instead, organisations should establish one security workstream that defines common principles across the Oracle Cloud estate.

This creates consistency while allowing each application to implement security in a way that reflects its specific business processes.

Whether designing procurement approvals, budget governance or financial close controls, the underlying governance principles remain the same.

Security Doesn't End at Go-Live

One of the most common mistakes is assuming security is complete once users can successfully access the system.

In reality, go-live marks the beginning of operational security.

- Users join and leave the organisation.
- Responsibilities change.
- Business structures evolve.
- Oracle introduces quarterly updates.
- New functionality is enabled.

Without ongoing governance, security gradually drifts away from the original design.

A dedicated security workstream should therefore extend beyond implementation and establish the processes required for:

- User lifecycle management
- Quarterly access certification
- Segregation of Duties reviews
- Privileged access monitoring
- Oracle quarterly release impact assessments
- Security optimisation
- Continuous compliance

Security is not a milestone.

It is an operational capability.

What a Dedicated Security Workstream Should Deliver

A mature Oracle Cloud Security workstream should provide far more than role configuration.

It should establish a structured delivery methodology covering:

- Security governance and operating model
- Business responsibility and persona analysis
- Role design principles
- Segregation of Duties assessment
- User provisioning strategy
- Identity integration
- Data security model
- Security testing
- Cutover planning
- Operational security governance

This ensures security remains aligned with business objectives throughout the implementation lifecycle, not just at go-live.

Building Security Into the Programme From Day One

The most successful Oracle Cloud implementations don't treat security as a technical dependency.

They treat it as a business workstream with its own governance, deliverables and accountable stakeholders.

When security is embedded from the beginning, organisations gain more than compliant access controls.

They create a platform that is easier to govern, simpler to maintain and better prepared for future growth.

Final Thoughts

Every Oracle Cloud implementation includes workstreams for finance, procurement, integration, testing and data migration.

Security deserves the same level of planning, governance and executive attention.

Because security influences every business process, every approval workflow and every user who interacts with the platform.

Treating it as a dedicated workstream doesn't add complexity.

It reduces risk.

And it creates a stronger foundation for long-term operational success.

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 believe Oracle Cloud Security should be delivered as a dedicated business workstream, not a technical task. By embedding governance, role design, Segregation of Duties and operational security throughout the implementation lifecycle, organisations build platforms that are secure, scalable and ready to support change long after go-live.

Because successful Oracle Cloud Security isn't delivered at the end of an implementation, it is designed into the programme from day one.

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