



Security Isn't About Roles
It's About Business Governance

Oracle enforces security decisions. It doesn't make them. Governance has to come first — roles come last.

ROLES
"Which Job Role should this user have?"

GOVERNANCE MUST ASK:

- ✓ Who owns this business process?
- ✓ Which duties require independent approval?
- ✓ What should never sit with one person?
- ✓ What authority level is appropriate?
- ✓ Who should access this data?

Oracle Cloud Security Isn't About Roles. It's About Business Governance

When organisations invest millions implementing Oracle Cloud Applications, most expect security to be one of the final technical workstreams before go-live.

- Roles are configured.
- Users are provisioned.
- Access is tested.
- The project moves into production.

Unfortunately, that's exactly why many implementations inherit security problems that become increasingly expensive to resolve.

The reality is that Oracle Cloud Security isn't primarily a technical exercise. It is a business governance exercise that happens to be implemented through Oracle's security model.

At Sarrisco, we've developed an Oracle Cloud Security Governance & Delivery Framework that helps organisations design security as part of the operating model, not as an afterthought. The framework provides a structured methodology covering Oracle Fusion ERP, Supply Chain Management (SCM), Oracle Enterprise Performance Management (EPM) and Oracle Identity & Access Management (IAM), ensuring security decisions remain aligned across the entire Oracle Cloud landscape.

The Problem with Traditional Security Projects

- Security is often introduced late in an ERP programme.
- Business process design has already been completed.
- Organisation structures have already been agreed.
- Approval workflows have already been configured.

Only then does someone ask the Security Lead to "create the roles."

By this stage, many of the most important security decisions have already been made, without considering governance, segregation of duties or long-term operational ownership.

The result is often predictable:

- Excessive access permissions
- Complex custom roles
- Segregation of Duties (SoD) conflicts
- Difficult quarterly Oracle updates
- Growing administrative overhead
- Audit findings that could have been prevented through better design

Security becomes something the organisation has to manage rather than something that actively protects the business.

Oracle Security Begins with Business Responsibilities

One of the biggest misconceptions is that Oracle security starts with Job Roles.

It doesn't.

It starts by understanding how the business operates.

- Who creates suppliers?
- Who approves purchase orders?
- Who prepares journals?
- Who approves budgets?
- Who certifies reconciliations?
- Who maintains enterprise metadata?

These are governance decisions, not Oracle configuration.

Only once these responsibilities are agreed should they be translated into business roles, Oracle Job Roles, duty roles, data security and workflow approvals. This business-led approach creates a security model that is easier to understand, easier to govern and significantly easier to maintain throughout the application lifecycle.

Security Across the Entire Oracle Cloud Estate

Modern Oracle programmes rarely stop with ERP alone.

Many organisations operate an integrated Oracle Cloud platform that includes:

- Oracle Fusion ERP
- Oracle Fusion Supply Chain Management (SCM)
- Oracle Enterprise Performance Management (EPM)
- Oracle Identity & Access Management (IAM)

Each application introduces different security requirements, yet the governance principles remain the same.

- Users should only receive the access necessary to perform their responsibilities.
- Segregation of Duties should prevent incompatible activities.
- Approval workflows should provide independent oversight.
- Business ownership should drive every security decision.

By applying a consistent governance model across ERP, SCM and EPM, organisations create a single security strategy rather than multiple disconnected security models.

Why EPM Deserves Equal Attention

Enterprise Performance Management is often overlooked during security design.

However, EPM contains some of an organisation's most sensitive financial information, including budgets, forecasts, financial close activities, reconciliations and enterprise metadata.

- These processes require exactly the same governance discipline applied within ERP.
- Budget preparation should remain separate from budget approval.
- Journal preparation should remain separate from journal approval.

- Financial close should include independent reconciliation and certification.
- Enterprise metadata changes should follow formal approval and deployment processes.

When EPM is treated as an extension of the overall security framework, organisations achieve consistent governance across operational and financial planning processes rather than managing separate security approaches.

Segregation of Duties Is a Business Decision

One of the most important principles within our framework is that Segregation of Duties is established within business processes, not within Oracle itself.

- Oracle enforces security.
- The business defines it.

Take Procure-to-Pay as an example.

A well-designed process separates supplier creation, supplier approval, purchase order creation, purchase order approval, goods receipt, invoice processing and payment execution between different business responsibilities.

Oracle then provides the technical controls to enforce those decisions.

This distinction fundamentally changes how organisations approach security and significantly reduces operational risk.

Security Doesn't End at Go-Live

Many implementation projects conclude once users can successfully log in.

We believe that's where operational security begins.

Security should continue throughout the lifecycle of the Oracle platform through regular access reviews, SoD assessments, privilege reviews, dormant account monitoring, Oracle quarterly update impact assessments and continuous optimisation.

As organisations evolve, security must evolve with them.

Treating security as an ongoing governance capability, not a one-time implementation task, helps maintain compliance while supporting future growth.

A Structured Delivery Framework

Our Oracle Cloud Security Governance & Delivery Framework provides a repeatable methodology covering every stage of implementation, including:

- Security governance
- Business process and persona analysis
- Role design
- Segregation of Duties assessment
- Security build and configuration
- Security testing
- User provisioning and cutover
- Operational security and continuous compliance

This structured approach enables organisations to establish secure, scalable and maintainable access across Oracle Cloud Applications while reducing implementation risk and supporting long-term operational governance.

Final Thoughts

Oracle Cloud Security should never be viewed as the process of creating Job Roles.

It is the governance of business responsibilities, business processes and organisational risk, implemented through Oracle's security model.

When organisations start with governance rather than configuration, they create security that is easier to explain, easier to operate and easier to audit.

At Sarrisco, that's exactly how we approach every Oracle Cloud implementation.

Because security isn't just about getting users into the system.

It's about ensuring the right people have the right access, at the right time, for the right reasons.

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