P-052020

JDE 101: Security Edition

BLUEPRINT 4D

May 4-7, 2026
Hilton Anatole in Dallas TX

Agenda

1. You Might Know less than you think
2. The Security Model – what it covers
3. SoD: Where many get it wrong
4. Privileged Access
5. Access Reviews Done Right
6. The Tooling Conversation
7. What Auditors are Looking for

We Help Our Customers Realize IT

Cloud Hosting

Public, private and hybrid cloud solutions

Managed Services

ERP system management with first-rate response times

AI and Gen AI

Integrating your business data with emerging technologies

JDE Consulting

Develop, implement, and support JDE applications

EPM Services

EPM consulting, advisory, and managed services

ERP Suites Services

Business Advisory Services

- Risk Management
- Technical Strategic Road mapping
- Enterprise Architecture Strategy
- Systems Gap Analysis
- Process Engineering
- Organizational Change Management
- Digital Transformation
- Analytics & Insights Strategy

Functional Consulting Services

- **JDE Security & Compliance**
- JDE Distribution & Warehousing
- JDE Manufacturing
- JDE Financials
- JDE Human Capital Management
- Managed Services
- UXOne & UDO Expertise
- Orchestration Design & Build

Technical and Infrastructure Services

- Technical Refresh
- Technical Upgrades
- Cloud Migrations
- IBM iSeries Administration
- Cloud Administration
- Networking & Server Infrastructure
- Identity Management
- Cybersecurity

erp suites

What’s New at ERP Suites

EPM Practice

Connects finance, operations, and strategy for one source of truth. It enables faster month end cycles and more accurate forecasts.

AI Agents

Goal-driven digital workers that plan and execute tasks inside JDE

JDE License Resellers

Proactively manage licensing changes, ensuring renewals, purchases, and adjustments stay compliant, and cost-effective.

Executive Summary

- **JDE Security is more complex than it appears**
- Most security has never been revisited post implementation and the gaps that create real audit exposure are rarely the obvious ones.
- Effective security is intentional
- You need to challenge your assumptions on security, access, and governance

You Might Know Less Than You Think

Effective Access

A user's real access is the sum of ALL roles assigned — not what any single role was designed to give. Can you easily answer, 'what can this user actually do?' without a third-party tool?

Menu Security leaks

Securing a menu does NOT prevent access to its applications. Users can reach those apps through another menu or a program exit. Menu-based security models are incomplete by design.

*PUBLIC – Silent Access

Any object not explicitly secured falls through to *PUBLIC. Do you know what *PUBLIC can do in your environment right now? If you don't have a *ALL restriction, then your door is wide open!

The Conflict Trap

Security settings in one role may conflict with the settings in another role. Role hierarchy determines which is effective. Does your design account for this?

erp suites

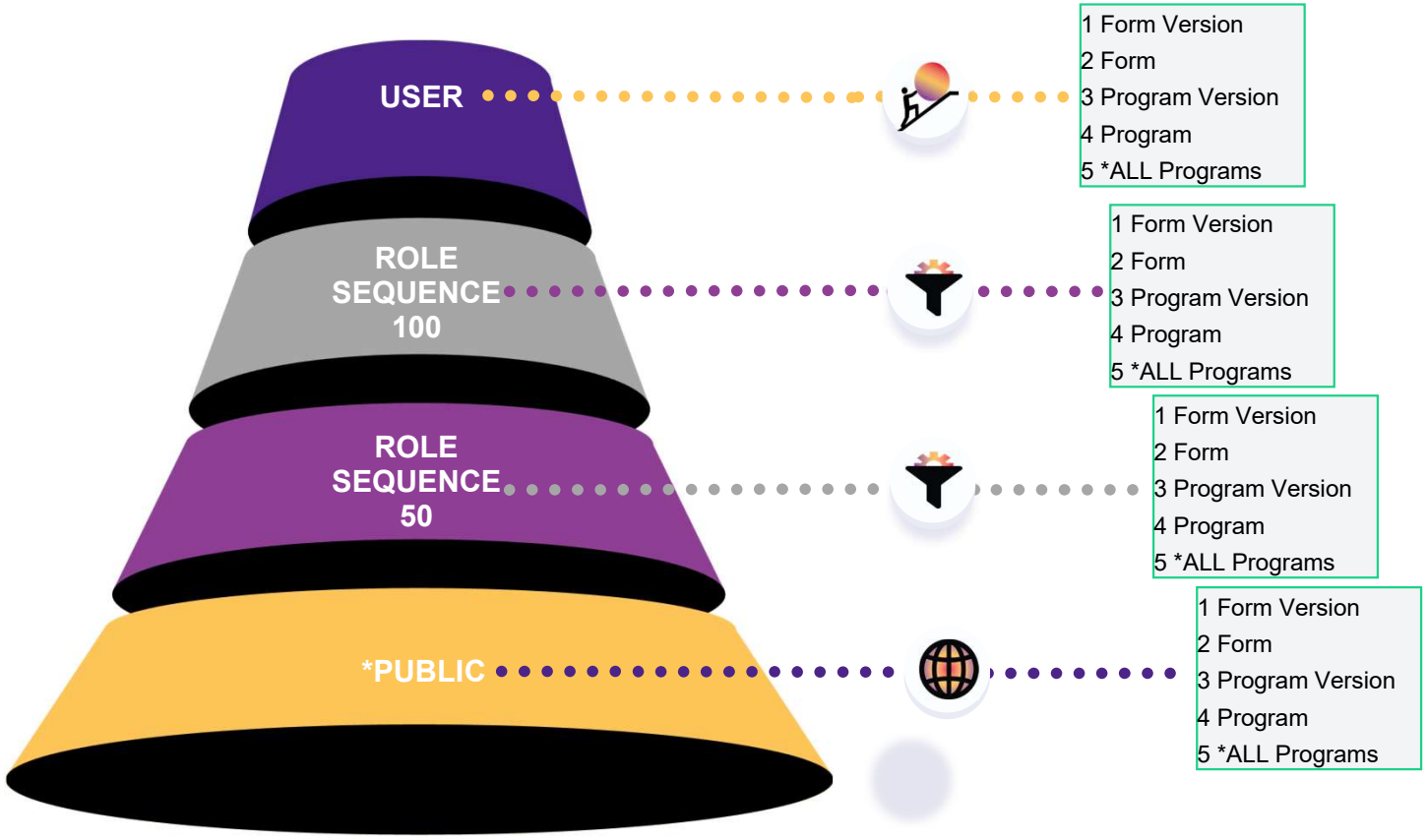
Security Model – All Four Layers

	Layer	Tool	What it Controls	Common Gaps
1	Application/Action/Processing Option Security	Security Workbench	Programs, Forms, Actions, UBEs, Data Selection	Over-permissive defaults, object descriptions mislead, unknown UBE function
2	Row/Column Security	P00950 Row & Column Security	Which data records a user sees and can transact against	Often skipped entirely – confusing to admins, invisible to users
3	*PUBLIC	JDE Default Security	JDE All users by default	Rarely audited or reviewed, default open access
4	Database Layer	DBA / OS credentials	DB Tables directly – bypasses JDE	Circumvents every control you've built

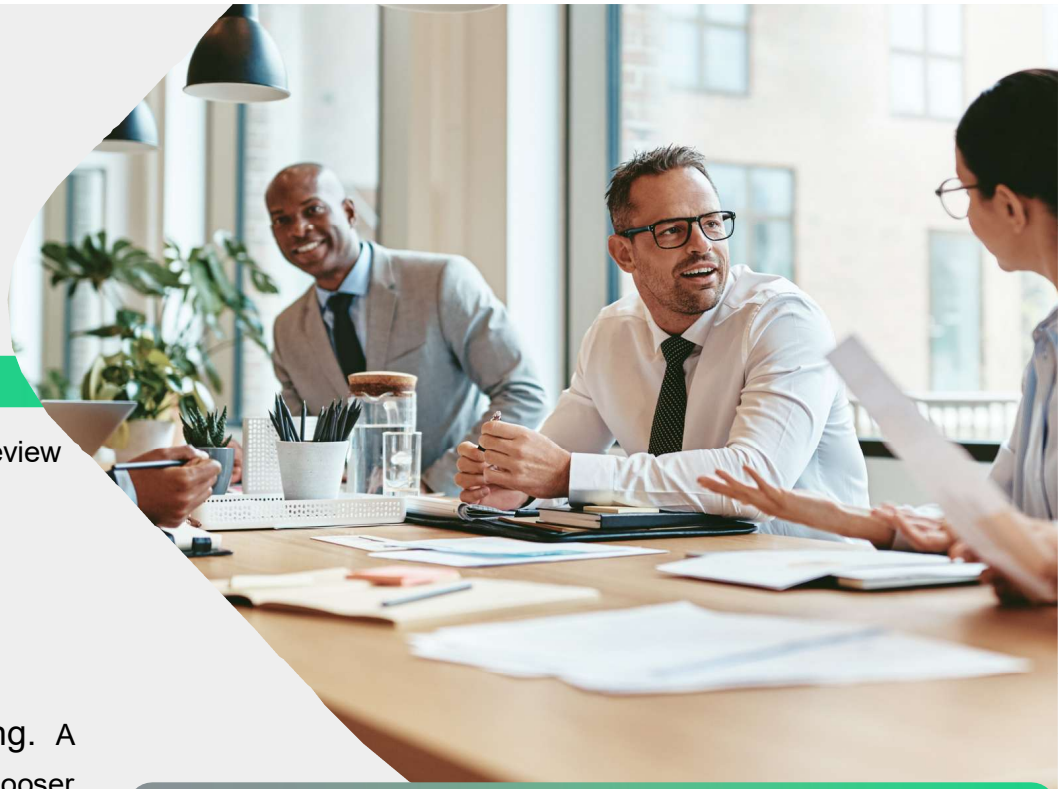
⚠ Critical: Database-level access bypasses every control you've built in JDE. If DBAs can touch SY920 or PRODDTA directly, your application security model has a floor missing.

erp suites

Security Hierarchy



Segregation of Duties (SoD)



- **Object descriptions Lie.** P0911B is labelled as GL Journal Review – sounds read only but it's not. Your SoD is only as good as your understanding of what each object actually does.
- **Your Rule set Goes Stale.** Custom programs, upgrades, new modules. A rule set built 3 years ago is a historical artifact
- **Role Sequencing & Role Chooser Change everything.** A role-by-role analysis misses the effect of sequencing and role chooser on effective access. You can pass a review and still have a conflict no one sees.
- **Native JDE has NO SoD Management.** There is no native functionality to manage SoD or compliance reporting. Manual processes with spreadsheets are unreliable at scale. This is not an opinion, it's a product limitation

SoD helps leadership understand where the business risk is and how to course-correct.

ALLOut Partner

erp suites

Privileged Access

Default System IDs

JDE ships with system user IDs — including "JDE" — with predefined, widely known passwords. If they haven't been changed, you have a critical exposure. Check both the front-end application AND the database

Shared Admin Accounts

Three people sharing one security admin account means accountability for none of them. When something changes, you can't prove who did it. Separate credentials, separate audit trails

Batch, Project, & Integration Users

Almost always over-privileged. Almost never reviewed. These accounts run silently in the background and are frequently granted broad access at implementation — then forgotten.

The ‘All Doors Open’ Default

JDE is delivered with allow everything. Many older environments were stood up this way and never properly secured. The residue is still there.

Access Reviews Done Right

Closed – what most companies do	vs	Complete – what auditors expect
Routed to managers	Exported role list	Routed to Managers with a deadline
Review closed after ‘enough’ managers responded	No response	Non-responses escalated – review doesn’t close until all responses received
No manager sign-off	Exceptions	Exceptions noted with compensating controls or remediation plan
80% reported as 100%	Coverage	100% actual coverage
No follow-up	Unresolved items	none
Last change to security	Security Changes	ALL Security changes tracked before and after the review cycle including what changed

erp suites

The Tooling Conversation

Native JDE Tools

- Security History (who changed what) little to no detail
- P00950 Security Workbench. Effective but time consuming
- F00950 table auditing is manual
- Simple Reporting

- **Answers basic questions only**
- **Doesn't scale, no SoD capability included**
- **No workflow, no automation**

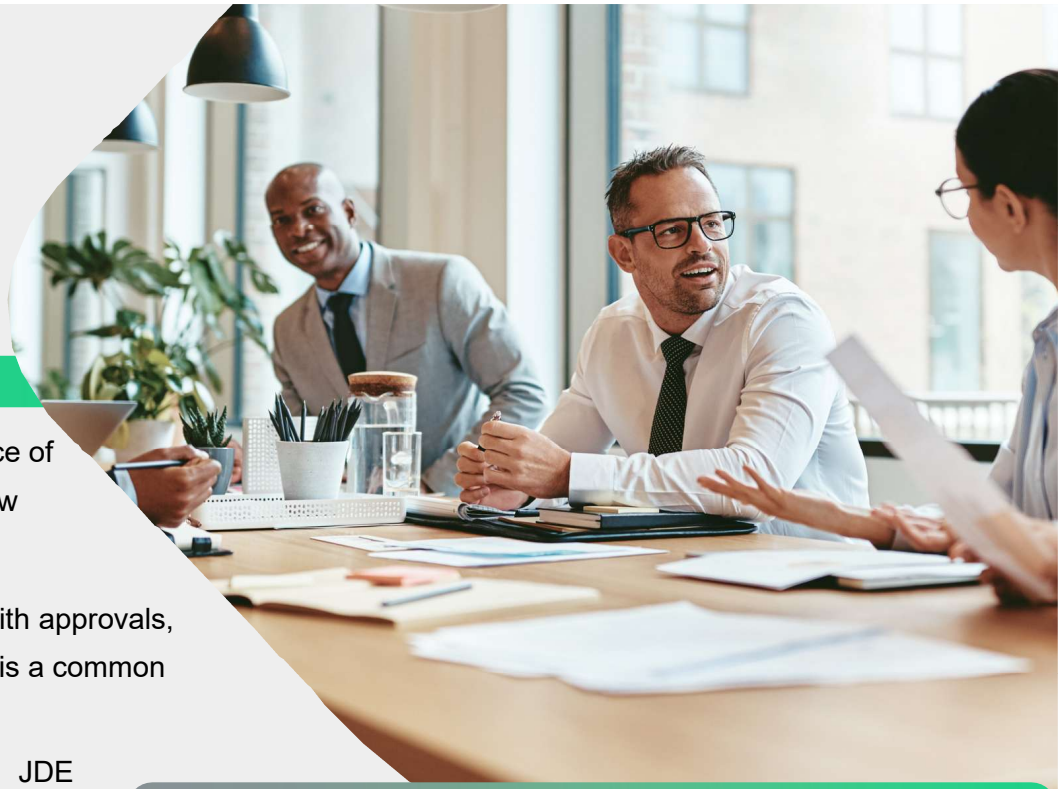
Third Party Solutions

- **ALLOut Security**
- *JDE-specific; SoD, cross-application SoD, security & role change control with SoD validation workflows and promotion audit trails, access reports, security management, menu management, user provisioning workflows, security history with before and after audit changes and reporting*
- **Qsoftware or SafePaas**
- *SoD, provisioning workflows, access reviews*

Take home question: Is your current process repeatable, defensible, and documented or is it heroics?

ALLOut Partner

What Auditors Are Looking For



- Show me your access review process. They want evidence of process: dates, manager names, & documented sign-offs. A review that just closed is not the same as a review that completed.
- Who approved this user's access? Provisioning requests with approvals, tied to a joiner/mover process. Documentation beyond 18 months is a common gap.
- How do you detect unauthorized changes? Native JDE captures basic activity. Direct DB changes are a blind spot. If your control is quarterly reconciliation, say so and be able to prove it's running.
- What SoD conflicts exist and how are they managed? They expect a current SoD matrix AND evidence of mitigating controls that are operating. Policies without evidence of execution will fail this test.

Oracle licensing audits are a growing risk with 62% of organizations reporting an audit in the last year.

erp suites

The Challenge

You probably came in today thinking your JDE security is pretty good.

The question isn't whether you have controls.

It's whether you can prove they work

and whether you'd know if they didn't.

Key Takeaways

- RBAC=Effective/Intentional Access
- Reviews need evidence
- Privileged Access is a real risk
- Native tools don’t scale
- SoD rules go stale
- Prove it. Don’t just say it.

erp suites


THANK YOU