INFOCUS 2026 · DENVER · SESSION P-053056

The Hidden Integration Tax

and the loophole you can take advantage of

Your access model decides whether absorbing an acquired company is a mapping exercise or a user-by-user rebuild.

Brian Connor

JD Edwards Risk Management · ERP Suites

The tax is documented, and it is expensive

$350M

Verizon / Yahoo, 2017

Purchase price cut from ~$4.83B to $4.48B after two breaches were disclosed mid-deal. About 7.2% of deal value. Verizon opened at $925M.

£18.4M + $52M

Marriott / Starwood

ICO penalty of £18.4M on 30 Oct 2020, down from a proposed £99.2M. Then $52M to 49 states and DC in Oct 2024, plus a 20-year FTC order.

53%

Forescout, 2019

Of 2,700+ decision makers across seven countries, 53% hit a critical cyber issue during a deal that put the deal in jeopardy. 65% reported buyer's remorse.

None of those three numbers were caused by a JDE role catalog. Which brings me to the part of this hour where I tell you why you should still be in the room.

A regulator named access controls, by name

> **"Failed to implement appropriate access controls.** For example, on numerous occasions, the accounts of former employees were not terminated in a timely manner, and separate unique accounts for users' remote access on Respondents' networks were not created."
>
> *FTC complaint against Marriott International and Starwood Hotels, October 2024, paragraph 27(d)*

Read what that paragraph actually names:

8	**Orphaned accounts** Former employees not terminated in a timely manner.
4	**Non-unique accounts** Separate unique accounts for remote access were not created.

Two rows of the scorecard you are holding, named by a federal regulator, in the highest-profile M&A security case of the last decade.

What these cases do and do not prove

WHAT THEY PROVE

- The integration tax is real, documented, and paid in cash.
- Security findings move purchase prices and survive for years after close.
- Regulators name access controls, orphaned accounts and shared credentials specifically.
- Acquirers routinely discover the problem after signing.

WHAT THEY DO NOT PROVE

- That role sprawl cut a purchase price. Yahoo was breach disclosure.
- That a permissive *PUBLIC stalled an integration. Marriott was an inherited compromise.
- No public case isolates the ERP access model as the variable. I looked. If you have one, find me afterward.

So here is the claim I will actually defend: the tax is real, and the access model is the part of it you own.

Before I earn the hour

The strongest argument against everything I am about to say, and where my boundary is.

Almost nothing that decides integration speed is decided in this room

Deal thesis, culture, talent retention and master-data quality are owned by the deal team, the CIO, the CFO and HR. Access and SoD is a real, ownable, value-protecting workstream. It is a supporting workstream. It is not the headline.

Who actually owns the levers

Deal thesis	Culture and retention	Master data quality	Access and SoD model
Deal team	CEO / HR	CIO / data owners	**You**

If I position a clean access model as the primary lever on deal outcomes, you should discount me. So I will not.

The defensible claim

NOT THIS: ~~"A clean access model accelerates M&A."~~

THIS: The access model is the difference between provisioning the combined workforce safely in weeks, and firefighting toxic access and audit findings for two quarters.

Narrower. Still worth an hour. And unlike the first version, I can defend every word of it.

Where my boundary is

MINE

- JDE role design and naming standards
- Process-aligned role catalogs
- SoD analysis, remediation, conflict matrix
- Security assessment: orphans, duplicates, *PUBLIC posture, environment scoping, signon
- SOX and ITGC as they apply to JDE access
- Security model documentation and KT
- PII and bank account masking
- ALLOut / Pathlock / Q Software tooling and licensing inside JDE

ADJACENT

- SAP GRC, Oracle Fusion Risk Management, Dynamics: methodology mine, platform partnered
- IAM and identity lifecycle: design mine, Okta / SailPoint / Entra execution partnered
- The access and SoD slice of cyber due diligence
- Access and security chapters of an M&A IT playbook
- Master data governance

NOT MINE

- Network, endpoint and cloud security
- Penetration testing and breach forensics
- Cultural integration and org design
- Financial, legal and deal structuring
- Application development and code migration

"The principles transfer. The mechanics do not, and I am not going to pretend I can configure your SAP GRC ruleset."

Map-ready, or rebuild-bound

Two patterns. One makes an acquisition a mapping exercise. The other makes it a user-by-user rebuild.

Two patterns

PATTERN A

Map-ready

- Closed-model *PUBLIC baseline
- Security at role level, not user level
- Roles grouped by function, sequenced deterministically
- Roles named and scoped to business processes: P2P, O2C, R2R
- SoD ruleset runs as a gate before provisioning

The work is: map job functions to existing roles, test the proposed assignments, resolve exceptions. Fast, and auditable.

PATTERN B

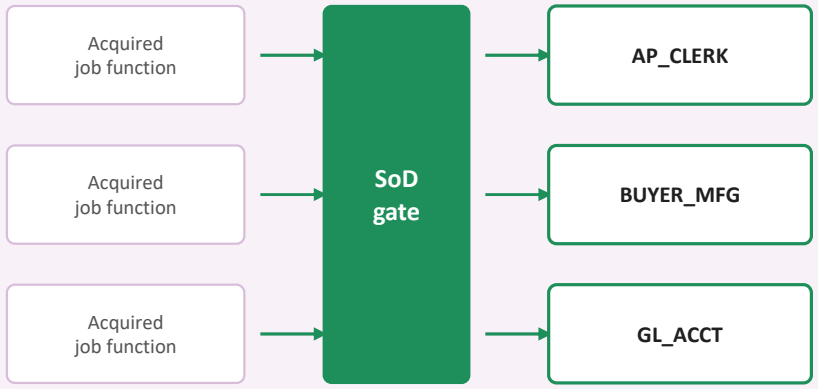
Rebuild-bound

- Permissive *PUBLIC granting broad access by default
- Security applied through user-level overrides
- Role precedence never governed, so resolution is unpredictable
- No naming standard. Environment and pathcode role drift
- Accumulated one-off grants nobody can reverse-engineer

There is nothing clean to map into. Every acquired user is a custom build, and you inherit their latent conflicts on top of your own.

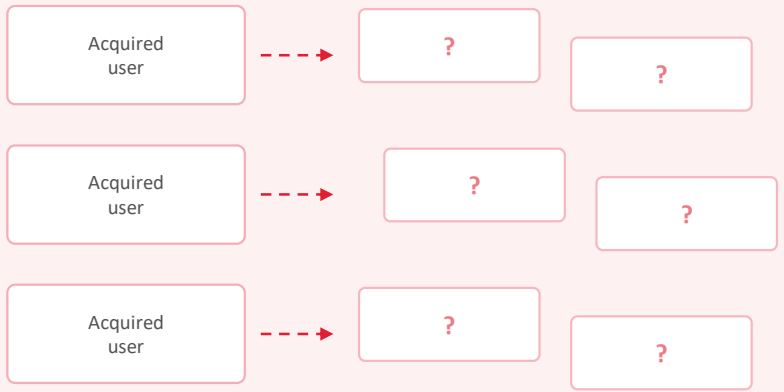
Map onto a model, or rebuild for every user

MAP-READY



Named roles. Bounded answer set.

REBUILD-BOUND



No gate. No named target. Unbounded.

The difference is not effort. It is whether the destination exists before the deal does.

I could not find a verifiable, named, public JDE M&A case that isolates the access model as the variable.

What follows is architectural reasoning at moderate-to-high confidence, plus composite experience from security assessments. It is not a citation, and I am not going to dress it up as one.

If you have such a case, find me afterward. I want it.

Eight checks

What absorb-ready actually looks like. Every one of these is a row on the handout.

The baseline: what everything else inherits

SCORECARD 3 4

3 *PUBLIC grants inquiry only

A permissive *PUBLIC is not a convenience. It is a standing grant to every user you will ever create, including every user you inherit on day one of an integration.

You are not securing users. You are securing the default that every future user starts from.

4 Role level, not user level

User-level security records are the single most corrosive pattern for absorbability, because they are invisible to a role-based mapping exercise.

You cannot map what is not in a role.

What a closed model actually buys you

up to

75%

reduction in critical SoD conflicts, immediately

Composite across the closed-model implementations we have run.

THE HONEST CAVEAT, AND SAY IT FIRST

Implementing a closed model does not always reduce record counts, especially coming from an open model. If someone promises you a smaller F00950, ask what happened to effective access.

WHAT IT DOES BUY

- Intentional, process-based access instead of accumulated grants
- A dramatic and immediate cut in critical SoD exposure
- A model an acquired workforce can actually be mapped onto

Row count is a maintenance metric. Critical SoD is a risk metric. Only one of them is worth reporting upward.

Two rules decide what a user can actually do

Reference slide. Everything on it follows from these two rules.

RULE 1 Levels are checked in order, and the first hit wins

Checked first

Only if no user record

The floor, for everyone

A setting at a higher level makes the lower levels invisible. One user-level record silently switches off every role and *PUBLIC control you built for that object, for that person, with no warning.

RULE 2 Among roles, the numerically higher sequence number wins

That is the whole lever. If you decide what the sequence numbers mean, you decide what wins. If you never decide, the winner is whatever order the roles happened to be created in.

Oracle, JD Edwards EnterpriseOne Tools Security Administration Guide 9.2

Sequence roles by function, not by accident

This is the part worth writing down.

Add, Change, Delete	`4000 – 4999`	*Most permissive. Wins.*
Add & Change	`3000 – 3999`	
Add	`2000 – 2999`	
Inquiry	`1000 – 1999`	*Least permissive. Yields.*

higher number wins

WHY IT WORKS

Rank the bands by permissiveness and the most permissive role a person legitimately holds is the one that resolves. The outcome is predictable before you provision, not discovered afterward.

WHAT DOES NOT HELP

Random role sequencing based on when the role was created. Resequencing roles to resolve a conflict.

This framework, on a baseline architecture for *PUBLIC and all roles, eliminates roughly **90% of role conflicts.**

The map, and the gate

SCORECARD 1 2

1 The role catalog

- Named for processes, not for people
- Not for departments, which reorganise
- Not for the role it was copied from
- Grouped by function, so the sequence bands mean something

The single highest-leverage acquirer-side item, and the only one on the scorecard you cannot buy.

2 SoD before provisioning

Simulate the access before you grant it. Importing acquired users into a clean role set is fast. Importing them into a sprawling model imports their conflicts plus yours, onto the audit critical path, and you find out from the auditor.

A quarterly detective report cannot gate anything. During an integration you provision hundreds of users in weeks.

Hygiene, paper, and the awkward one

SCORECARD 6 7 8

6

Licence transferability and change of control

- The awkward one, and the one nobody puts on a security slide.
- Non-transferable licences and change-of-control fees are a named diligence red flag, and this applies to your JDE security tooling itself.
- The space has consolidated. Read the terms before a deal makes you read them.

7

Documented, not tribal

- Diligence treats security knowledge concentrated in one or two people who are not on retention agreements as a defect.
- Say this one plainly: if you are the only person who knows why role X exists, you are a diligence finding.

8

Orphans, duplicates, privilege creep

- Documented diligence red flags: orphaned accounts, contractors with standing access, no MFA on admin and email, broad local admin.
- Each one lowers the price or stalls the close.
- Duplicates are pure cost: they inflate F00950 and slow SoD reporting.

Six tables, 19 queries.

TABLE	WHAT IT HOLDS	WHAT TO LOOK FOR	THE BAD ANSWER
F00950	Security Workbench	*PUBLIC grants by security type, and the count of user-level records	*PUBLIC granting add, change or delete. A large user-level record count.
F00926	Role Sequence	Roles grouped by function, each function in its own band	Numbers that mean nothing, so nobody can predict which role wins
F95921	Role Relationships	Volume of role assignments, active against expired, and roles per user	Expired assignments never removed. Users carrying roles nobody can justify.
F0092	User & Role	The full inventory of users and roles. It will not tell you who is active	Profiles nobody recognises, and service accounts set up as people
F0093	Environment List	Which roles can reach production	Roles designated non-production that carry production access
F98OWSEC	Sign-on security	Active, disabled and locked-out users; password change frequency and attempt limits	Passwords that never expire, and accounts that never lock

***PUBLIC volume is not the metric.** 500 to 1,000 records is normal depending on the modules you run, and every search, select and inquiry program should be there. What matters is whether *PUBLIC grants anything beyond inquiry.

A tool is a force multiplier on a target model

ALLOut will not tell you what your roles should be. What it will do, once the model exists, is show you continuously whether the model is still holding. For this audience that is the part that matters.

Three things worth a licence, and none of them are bulk editing

1

Overview of the system

One place that answers “what does our access risk look like right now”, instead of six exports and a spreadsheet.

2

Access controls

Who can reach critical programs, what changed, who approved it, and whether provisioning followed the model.

3

Compliance

Evidence produced as a by-product of running the controls, rather than assembled the week before the auditor arrives.

During an integration this stops being a convenience. You are provisioning at ten times normal rate into a model you are still proving.

What that looks like: the dashboards

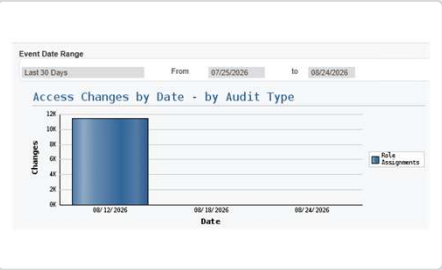
SoD by role and user

Where the conflicts are, and whose access creates them.

Security changes

What changed, when, and by whom.

User provisioning and changes



Whether new access followed the model or went around it.

Access to critical programs

Who can reach the things that move money.

The reports already exist. The dashboard is for the person who has to decide something, and every chart and every figure is clickable straight down to the detail record.

Overview when you want the shape of the risk. Drill-down when you need the record. The same data, two audiences, no second export.

The loophole

How work that nobody will fund as M&A prep gets funded anyway.

Why nobody funds M&A readiness

No deal yet

There is no budget line for integration until a deal is live. “It might help with a hypothetical future acquisition” has never won a funding argument.

→

Deal announced

Budget appears. So does the clock. You are now provisioning at 10x normal rate into whatever model you already had.

→

Window closed

The readiness work you needed had to happen before the deal. By the time it is fundable, it is too late to do it.

Stop trying to sell it as M&A prep. It is an argument you will lose, and you should lose it, because the objection is correct.

The work that accelerates a future integration is the same work that passes a SOX audit and reduces access risk today.

Fund it where the budget already exists.

Lead with the standalone compliance payoff. M&A acceleration is the second reason, never the first.

It is not a rhetorical trick. Check the mapping.

1	**Documented, process-aligned role catalog**	→ Access control design and documentation	5	**Roles sequenced in function bands**	→ Deterministic, evidenced access resolution
2	**SoD analysis before provisioning**	→ Preventive segregation of duties control	6	**Licence transferability mapped**	→ Vendor and contract management
3	***PUBLIC grants inquiry only**	→ Least privilege	7	**Security model documented**	→ Control documentation, key-person risk
4	**Role-level, not user-level security**	→ Role-based provisioning	8	**Orphan and privilege-creep cleanup**	→ Periodic user access review

There is no M&A-only line item on that list. That is the entire point.

Sequencing, and why the order is not arbitrary

1

Baseline first

Least privilege and role-level security. Nothing else works until the baseline is a closed model, because every later decision inherits it.

2

Function bands and the catalog

Group roles by function, band the sequence numbers, name the catalog. This is the asset, and the part you cannot buy.

3

Preventive SoD, and hygiene forever

The gate, plus the recurring reviews that keep the catalog from decaying back into Pattern B. This one never finishes.

Build the catalog before the baseline and you are defining roles on top of grants you are about to remove.

And the honest close: the access model is an accelerant, not the deal's success factor. Culture and talent retention dominate the outcome. A clean role design must not create false confidence that the hard parts are handled.

Map-ready, or rebuild-bound?

1	Documented, process-aligned role catalog with a naming standard	Y	N
2	SoD analysis run BEFORE provisioning, not discovered after the fact	Y	N
3	*PUBLIC baseline designed on purpose: inquiry granted, everything beyond inquiry denied	Y	N
4	Security applied at the role level, not through user-level overrides	Y	N
5	Roles sequenced in function bands, so the resolving role is predictable before you provision	Y	N
6	Software licence transferability and change-of-control mapped	Y	N
7	Security model documented, not held in one or two people's heads	Y	N
8	Recent orphan, duplicate, and privilege-creep cleanup completed	Y	N

SCORE KEY

7-8
Map-ready

4-6
Partial. Close the gaps before a deal lands.

0-3
Rebuild-bound. Start now.

The six tables and the SQL: pages 2-6.

Monday morning. Two numbers.

Count your non-unique users, and count your orphaned users.

Five counts in total. None of them need a baseline to interpret, and none of them need tooling.

1 Non-unique users

One login, more than one human behind it. Two counts.

1. Profiles with no address book link `ULAN8 = 0`
2. Address book numbers holding 2+ user IDs

A real person has an address book record. A generic or shared login usually does not.

2 Orphaned users

A login nobody owns. Three counts, not one.

1. Enabled, holding no active role
2. Enabled, no sign-in for 180+ days
3. No F98OWSEC record at all

These are not my two numbers. They are the ones the FTC named in the Marriott complaint.
The SQL for all five is on page 4, Oracle, or page 6, SQL Server. Four run as printed; the 180-day count needs sign-on history switched on.

The integration tax gets paid either way.

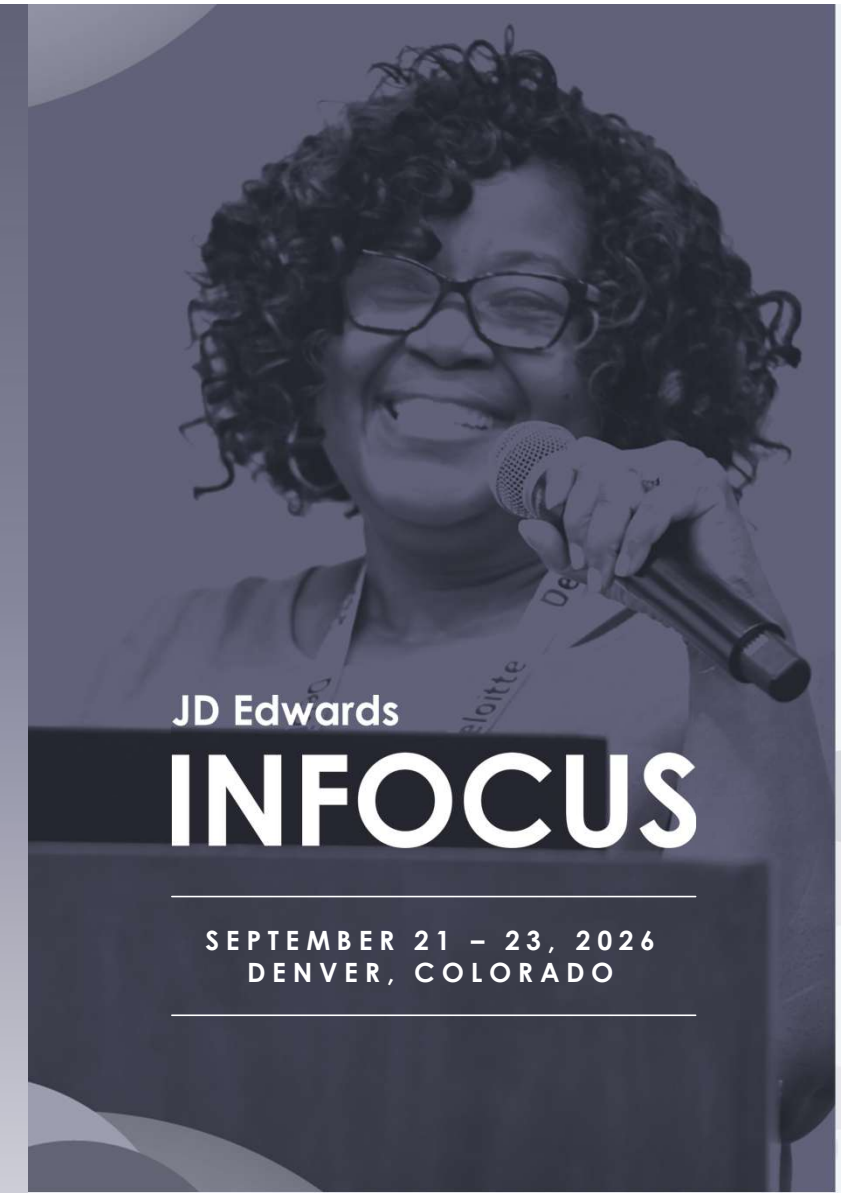
The only question is whether you pay it in advance, on your own schedule, out of a budget that already exists.

Brian Connor
JD Edwards Risk Management · ERP Suites

bconnor@erpsuites.com

Questions

Deck and resources



Q&A

Contact me:

Brian Connor

JD Edwards Risk Management · ERP Suites

bconnor@erpsuites.com

Session ID:

P-053056

Quest
JD Edwards
Community

erp suites