

BEYOND THE CRACKDOWN

The Shadow Estate: When the Workarounds Became the Architecture

A year of improvisation turned unsanctioned tools into load-bearing infrastructure — and the question is no longer how to eliminate it, but what to do now that we cannot.

Giovanni Leonardi

April 2021



Contents

1. Executive Summary	3
2. The month the map stopped matching the ground	3
3. How the exception became the rule	4
4. Two stories we tell, and why both mislead	4
5. What is actually out there	5
6. The debt beneath the debt	5
7. The reconquest reflex	6
8. From reconquest to stewardship	6
9. Now what	7

The Shadow Estate: When the Workarounds Became the Architecture

Transformation · No. 313

Originally written April 2021 | Re-edited and re-rendered for the WhereBeyond Edition, 2025

“The gap between forty and three hundred and eighty is not the residue of indiscipline; it is the accumulated record of a year in which people were asked to keep delivering, and did.”

1. Executive Summary

Over the past year, the improvised tools that individuals and teams reached for to keep working — the file-sharing accounts, the messaging workspaces, the spreadsheets that quietly became systems of record — stopped being exceptions and became the operational core. What we still call shadow IT has changed state: a manageable fringe has become mainstream infrastructure, and the vocabulary of exception no longer describes the reality. This essay argues that the instinct now taking hold — to reassert control by inventorying, consolidating, and shutting things down — misreads what happened and will fail for the same reasons the original controls failed. The year did not expose a discipline problem. It exposed a governance model built for a slower world. The more honest response is to treat what has accumulated as an estate: something to be surveyed, secured, and stewarded rather than abolished. That is a less satisfying answer than a crackdown, and it is the only one that holds.

2. The month the map stopped matching the ground

There is a particular meeting that recurs across organisations just now, and it has a recognisable shape. Someone — often the newly serious owner of information security, sometimes a finance lead chasing software spend — puts a single number on a slide. The number is the count of distinct cloud applications in active use across the organisation, assembled for the first time not from the asset register but from expense records, single sign-on logs, and network traffic. The register says one thing: perhaps forty sanctioned applications, tidily owned and licensed. The new number says something else entirely. I have watched a version of this meeting land on a leadership team, and the figure that silenced the room was three hundred and eighty. Not forty applications with a few rogue extras, but nearly ten times the estate that IT believed it was running — assembled quietly, department by department, over about twelve months.

The gap between forty and three hundred and eighty is the subject of this essay. It is tempting to read it as a failure of control, a lapse that a firmer hand would have prevented. That reading is comforting and wrong. The gap between forty and three hundred and eighty is not the residue of indiscipline; it is the accumulated record of a year in which people were asked to keep delivering, and did. When the formal systems could not absorb the disruption, the informal ones did, and they are still doing it now.

3. How the exception became the rule

Shadow IT is not new. For as long as central technology functions have existed, people have routed around them. The familiar version was marginal and slightly comic: a departmental database maintained by the one person who understood it, a team analytics tool bought on a corporate card, a mail rule doing the work of an integration. It irritated auditors and it stayed contained. What changed over the past year was not the impulse but its scale and its necessity.

The mechanism is not mysterious. The sanctioned path to a new capability ran through a request, a queue, a security review, a procurement step, and a provisioning window — and it measured itself in weeks. The workaround ran through a work email address and an invite link, and it measured itself in minutes. When the deadline was immovable and the two paths sat side by side, people chose minutes. They were not being reckless; they were being responsible to the thing in front of them. Multiply that single, rational choice across every team, every week, for a year, and you do not get a fringe. You get an estate.

The sanctioned path measured itself in weeks; the workaround measured itself in minutes. Given an immovable deadline, no volume of policy was ever going to make weeks beat minutes.

4. Two stories we tell, and why both mislead

The organisation tends to reach for one of two ready-made stories about all this, and the difficulty is that each contains just enough truth to be dangerous on its own.

The first is the control story. Shadow IT is risk: data leaves the boundary, obligations under data-protection law are breached without anyone deciding to breach them, and the attack surface expands invisibly. Every unsanctioned tool is a liability waiting to be discovered. This is true as far as it goes, and it goes further now than it used to. But held alone it misses the decisive fact — that a great many of these tools are no longer optional embellishments. They are load-bearing. Treating a system of record as a compliance nuisance to be switched off is a category error about what it has become.

The second is the innovation story. Shadow IT is grassroots progress: users voting with their feet for tools that work, exposing how slow and paternalistic the centre had become. There is truth here too — much of what people adopted was genuinely better than what they were offered. But held alone this story romanticises the mess. A system of

record that no one is accountable for, that has no backup and no access model and no one who can explain its logic, is not a triumph of user empowerment. It is a fragility dressed as a victory.

The essay's wager is that neither story is adequate because the phenomenon has outgrown both. We are no longer looking at deviance to be corrected or at rebellion to be celebrated. We are looking at infrastructure that arrived by the back door and now has to be run.

5. What is actually out there

It helps to be concrete about what the estate contains, because the abstraction shadow IT flattens a very textured reality.

- A spreadsheet that has quietly become the authoritative view of a core process — reconciliations, pipeline, headcount — maintained by one person, with a formula or macro that no one else fully understands.
- A customer list, or a supplier list, living in a personal cloud drive because that was the only place two people in different teams could both reach it in a hurry.
- A messaging workspace, adopted for speed, in which the real decisions of the organisation are now taken and recorded — outside every retention policy the organisation believes it has.
- A no-code app a capable colleague built to solve a workflow the core systems never handled, now depended upon by forty people who have never met its author.

Each of these is individually reasonable and collectively unmanaged. Consider the first at close range. In one finance function, the monthly close came to rest on a single workbook that one analyst maintained, complete with a macro she had written herself. When she took a fortnight's leave, the close slipped four days — not because the numbers were hard, but because the process lived entirely in her head and on her hard drive. Nobody had decided to make a person a single point of failure for the month-end. It happened one sensible shortcut at a time, and no one noticed until it had.

6. The debt beneath the debt

We have grown fluent in the language of technical debt — the future cost of present shortcuts in code and architecture. The shadow estate is a related but less discussed liability, and it deserves its own name: governance debt. Every workaround borrowed a little against a future reckoning. It borrowed clarity about who owns the data, certainty about where it sits, assurance that it can be recovered, and the plain knowledge of what exists at all. The interest on that borrowing did not show up while the pressure was on. It is showing up now, in the meeting with the number on the slide.

This is where the phenomenon connects to something larger and more uncomfortable: the distance between the transformation an organisation planned and the one it actually got. The roadmaps of the last few years promised modern, integrated, governed platforms. What people actually used, when it mattered most, was assembled from the

bottom up, in a hurry, from whatever was to hand.

“The shadow estate is the difference between the transformation that was on the roadmap and the transformation that actually happened.”

That gap is not a temporary aberration to be closed by returning to plan. It is the truest available account of how the organisation actually works. Any strategy that begins by wishing it away has already lost contact with the ground.

7. The reconquest reflex

The instinct, once the number is on the slide, is reconquest. Inventory everything. Consolidate onto the sanctioned platforms. Withdraw the tolerated tools and block the rest. Re-establish the tidy map of forty applications and hold the line this time.

I want to give this instinct its strongest form, because it is not foolish. Unmanaged tools are genuine exposure, and the exposure is not hypothetical. A regulator examining a data-protection failure does not accept our staff improvised as mitigation; the obligation sat with the organisation the whole time. Consolidation genuinely does reduce cost and shrink the attack surface. And someone must, in the end, be accountable for where the organisation's information lives. The case for pulling the estate back under control is serious, and I do not dismiss it.

But reconquest fails, and it fails for a precise reason: it repeats the original error. It assumes the central function can define, ahead of need, the full set of tools that every part of the organisation will require – and then enforce that definition. That assumption was already shaky before the disruption. It is untenable now, because the organisation has just spent a year demonstrating, at scale, exactly what people do when the sanctioned set does not meet the need. They find a window. Shut the estate down by decree and you do not eliminate the behaviour that created it; you drive it somewhere darker and less visible than the place it currently sits, where at least the expense records and the sign-on logs can still see it.

8. From reconquest to stewardship

The more durable posture is not reconquest but stewardship – the mindset of someone who has inherited an estate too large to demolish and must instead survey it, secure it, and gradually bring it into good order. It accepts the map has changed and sets out to govern the actual terrain rather than the remembered one.

In practice that reorders the work.

1. Survey before you judge. Make the invisible visible and keep it visible — the count on the slide should be a live instrument, not a one-off shock. You cannot steward what you refuse to look at.
2. Triage by load, not by origin. The question is not whether a tool was sanctioned but whether the organisation now depends on it. The load-bearing spreadsheet and the decision-making messaging workspace are the priorities; the harmless novelty can wait.
3. Bring the controls to the work. Extend identity, access management, and data protection outward to where people actually operate, rather than dragging the work back inside a boundary it has already left.
4. Adopt what earns adoption. Where a workaround is genuinely better, sanction it properly — give it an owner, a backup, a licence, a place in the register — instead of forcing people back onto the tool they fled.
5. Give the builders guardrails, not prohibitions. The capable colleague building no-code apps is an asset if bounded and supported, and a liability only if ignored until the app breaks.

Stewardship trades the satisfaction of a tidy map for the safety of an accurate one. It is the worse story and the better strategy.

None of this is as emotionally satisfying as a crackdown. A crackdown offers the fantasy of restored order; stewardship offers only the slow, unglamorous work of governing what is actually there. But the crackdown restores order on paper while the estate carries on in the shadows, and stewardship governs the estate as it is.

9. Now what

The title of this essay asks now what, and the honest answer is that the shadow estate is not a problem to be solved but a condition to be managed. The tools that went mainstream are not going back into the shadows, because they were never really in the shadows to begin with — they were in the daylight of everyone's actual working day, invisible only to the register that claimed to describe it.

The organisations that come out of this well will not be the ones that recover the cleanest inventory. They will be the ones that give up the memory of forty applications, accept the reality of three hundred and eighty, and get to work turning an accidental estate into a governed one. The job changed from prevention to stewardship somewhere in the middle of the last year. Most organisations have not yet noticed. The first step is to admit that the exception became the rule — and that ruling it is now the work.