

BEYOND THE QUICK FIX

The Technology Debt Accelerator — Quick Fixes That Became Permanent Architecture

A Practitioner's Perspective on the Hidden Cost of Emergency Digital Delivery

Giovanni Leonardi

June 2020



The Technology Debt Accelerator — Quick Fixes That Became Permanent Architecture

Transformation · No. 245

Originally written June 2020 | Re-edited and re-rendered for the WhereBeyond Edition, 2025

“The emergency architecture is not temporary. It is the new permanent, and nobody has approved it.”

1. The Speed That Felt Like Progress

Three months ago, most large organisations could not have imagined deploying enterprise-wide technology changes in a matter of weeks. The governance processes alone — architecture review boards, security assessments, procurement cycles, change advisory boards — would have consumed months before a single line of code was written. And yet here we are. Entire workforces shifted to remote collaboration platforms in days. Customer-facing channels that had been on eighteen-month roadmaps went live in three weeks. Backend integrations that had been deemed too risky to attempt were built, tested, and deployed over a long weekend.

The speed has been remarkable. It has also been celebrated — held up as proof that organisations can move fast when they have to, that bureaucracy was the real bottleneck all along, that the crisis has unlocked a capability that was always there. There is truth in all of this. But there is also something that almost nobody is talking about yet, and it is this: the technology decisions made under emergency conditions in the last ninety days are not temporary. They are hardening, right now, into the permanent architecture of these organisations. And the debt they are accumulating will take years to repay.

2. How Emergency Becomes Permanent

The pattern is well understood in engineering, even if it is rarely discussed in programme boards. When a system is built under extreme time pressure, certain compromises are made deliberately. Security controls are simplified. Data models are flattened. Integration patterns that would normally go through an API gateway are wired point-to-point. Authentication is bolted on rather than designed in. Logging and monitoring are left for later. Documentation is written in someone's head and nowhere else.

These compromises are rational in the moment. The alternative — taking the time to do it properly — was not available. The organisation needed to function, and the technology teams delivered what was needed to make that happen. The problem is what comes next.

In my experience, the half-life of a temporary solution in a large organisation is approximately forever. The moment a quick fix goes into production and people start

depending on it, a gravitational force takes hold. Users build processes around it. Other systems integrate with it. Business cases are written that assume its continued existence. The cost of replacing it grows with every passing week, while the urgency of replacing it — because it works, after a fashion — diminishes.

The most dangerous technology decision is not the one that fails visibly. It is the one that succeeds just well enough to become permanent before anyone notices it was never designed to last.

This is the dynamic now playing out across thousands of organisations simultaneously. The emergency deployments of March and April are, by June, no longer emergencies. They are infrastructure. They are being treated as baselines. And the technical debt they represent is being silently absorbed into the architecture without anyone having made a conscious decision to accept it.

3. The Anatomy of Pandemic Technical Debt

The debt being created is not uniform. It has a specific shape, driven by the particular pressures of the current crisis, and understanding that shape matters because it determines where the failures will eventually appear.

Security debt is the most acute. Organisations that spent years tightening perimeter security suddenly had to open access from thousands of unmanaged home devices. VPN concentrators were scaled by adding capacity rather than redesigning access patterns. Multi-factor authentication was relaxed for speed. Data loss prevention controls were quietly turned down because they were blocking legitimate remote work. Each of these decisions made sense in isolation. Together, they represent a systematic weakening of the security posture that will take far longer to reverse than it took to create.

Integration debt is the most structural. The point-to-point integrations built under pressure — direct database connections, file-based transfers, screen-scraping workarounds — have created a web of dependencies that no architecture diagram currently captures. When these integrations fail, and they will, the failure modes will be unpredictable because the integration patterns themselves were never formally designed.

Data debt is the most insidious. Rapid deployments rarely include data quality frameworks. Customer data has been captured through hastily built forms, migrated through manual processes, and stored in systems that were never intended to be systems of record. The inconsistencies being created now will surface months or years from now, in regulatory reports that do not reconcile, in customer communications that contradict each other, in analytics that tell stories that are not true.

Operational debt is the most underestimated. The teams that built these emergency solutions are the same teams that now support them. But the support model is informal — it lives in the institutional memory of the people who were in the room when the decisions were made. There are no runbooks. There are no documented recovery procedures. There is no capacity planning. When these individuals move on, as they inevitably will, the knowledge goes with them.

4. Why This Time Is Different

Technology debt is not new. Every organisation of any size carries it. What makes the current moment different is three things.

First, the scale is unprecedented. This is not one team cutting corners on one project. This is every technology team in every organisation making similar compromises simultaneously. The total volume of unplanned, unarchitected technology now in production across the global economy is something we have never seen before.

Second, the speed of accumulation has been extraordinary. Normally, technical debt builds gradually — a shortcut here, a deferred refactoring there, a library upgrade that never quite makes it to the top of the backlog. What has happened in the last three months is a step-change. Entire architectural layers have been built on compromises that would, in normal circumstances, never have passed review.

Third, and most critically, the organisational awareness is almost non-existent. In a normal technology programme, the team knows it is taking on debt. There is usually a conversation — however perfunctory — about the trade-off between speed and quality, and some nominal commitment to address the debt later. What has happened in this crisis is different. The debt has been taken on as a by-product of survival, and in many organisations nobody has yet paused to catalogue what has been built, assess its fitness for continued use, or estimate the cost of bringing it to a sustainable standard.

5. The Compounding Effect

Technical debt, like financial debt, compounds. A quick integration built in March becomes a dependency for a second system in April. By May, a third system is consuming data from the second, which relies on the first. By June, you have a chain of dependencies three layers deep, none of which was designed, all of which are in production, and the cost of unwinding any one of them has tripled because of what has been built on top.

This compounding is happening now, in real time, and it is accelerating. Every week that passes without a deliberate pause to assess and plan makes the eventual remediation more expensive and more disruptive. The organisations that will fare best are those that recognise this dynamic early enough to act before the debt becomes truly structural.

- The emergency VPN expansion that bypassed security architecture review is now the de facto access pattern for the entire workforce
- The customer portal built in two weeks on a prototyping framework is processing real transactions against production databases
- The collaboration platform deployed as a stopgap has become the primary channel for governance decisions, with no retention policy and no audit trail
- The data integrations built by hand during the crisis are now feeding regulatory reporting, and nobody has validated the transformation logic

6. What Needs to Happen

The first step is acknowledgement. Organisations need to accept that they have taken on a material volume of technology debt in a very short period, and that this debt is not self-correcting. Left unaddressed, it will degrade system reliability, increase security risk, and constrain the organisation's ability to change direction in the future.

The second step is assessment. Not a multi-month architecture review — the situation does not afford that luxury — but a pragmatic catalogue of what has been built, what state it is in, and where the highest risks lie. This means asking uncomfortable questions: which of the emergency deployments are still running on someone's personal credentials? Which integrations have no error handling? Which data flows have no validation? Where is the single point of failure that, if it goes down at two in the morning, nobody knows how to recover?

The third step is prioritisation. Not everything needs to be fixed immediately, and not everything needs to be rebuilt from scratch. Some emergency solutions will prove to be good enough with modest hardening. Others will need to be replaced entirely, but on a timeline that can be planned rather than forced by failure. The critical skill is distinguishing between the two — and having the organisational honesty to admit which is which.

The question is not whether organisations will pay down this debt. They will — either deliberately, through planned remediation, or involuntarily, through system failures, security breaches, and regulatory findings. The only choice is which.

7. The Transformation Paradox

There is a deeper irony here. Many of the organisations now accumulating emergency technology debt are the same ones that were, six months ago, running multi-year digital transformation programmes. Those programmes had governance. They had architecture principles. They had quality gates. And they were, in many cases, moving too slowly to deliver business value.

The crisis has demonstrated that the organisations can move fast. But it has also demonstrated the cost of moving fast without the structures that make speed sustainable. The transformation programmes of the future will need to find a way to preserve the urgency and decisiveness of the last three months while rebuilding the architectural discipline that was, quite reasonably, set aside.

That is a genuinely difficult problem. But it starts with being honest about where we are: standing on a foundation of emergency decisions that nobody intended to be permanent, watching them become permanent anyway, and knowing that the longer we wait to address this, the harder it will be.