# When Systems Forget the Mission

Modern technology systems were supposed to simplify institutions.

Instead, many institutions have become increasingly difficult to understand even for the people responsible for operating them.

Over time, layers of:
compliance,
outsourcing,
cloud infrastructure,
recurring licensing,
cybersecurity frameworks,
vendor ecosystems,
administrative process,
and institutional narrative management

have created environments where operational clarity is often replaced by abstraction.

The problem is not technology itself.

The problem is drift.

Systems originally designed to support human mission requirements slowly begin prioritizing process, presentation, defensibility, recurring revenue, and institutional self-preservation.

Meanwhile, the people actually carrying the mission increasingly struggle under the weight of the systems surrounding them.

The pattern now appears almost everywhere.

Police officers spend increasing amounts of time feeding reporting systems while departments struggle with staffing shortages.

Doctors spend enormous amounts of time fighting insurance systems over procedures eventually approved anyway. The American Medical Association has repeatedly warned that prior authorization systems continue creating growing administrative burdens while contributing to physician burnout and delays in patient care.

Teachers describe spending more time satisfying measurement systems than mentoring students.

Engineers warn about operational concerns while organizations face pressure tied to schedule, production targets, investor expectations, and quarterly reporting cycles.

A respected property manager with years of trusted service can suddenly find her standing threatened by one poorly considered survey score because a simplified metric begins carrying more weight than years of demonstrated judgment, patience, and operational competence.

This is how institutional trust erodes.

Not usually through one dramatic collapse.

But through thousands of small moments where systems stop seeing human beings clearly.

I have spent more than 25 years running a small IT consulting company called Hi5s, Inc.. During that time I worked with municipalities, police departments, medical practices, churches, and small businesses. Over those years I kept noticing the same pattern appearing again and again.

Systems built to support people slowly became systems people were forced to serve.

Years ago while working at Unisys, I watched the company distribute glossy employee "Flex Benefits" packages printed on expensive paper and presented in polished folders. The presentation looked optimistic and forward-thinking.

But many employees understood the underlying reality differently.

Benefits were shrinking.
Compensation lagged behind inflation.
Review cycles stretched longer and longer.

I remember quietly thinking:

Maybe spend less money selling the story and more money supporting the people actually carrying the mission.

That moment stayed with me for years because it revealed something larger than one company policy.

Institutions can slowly drift into environments where narrative management becomes more important than operational truth.

Not necessarily through conspiracy.

Not necessarily through evil intent.

But through gradual abstraction.

The people closest to operational reality increasingly lose influence while systems designed to measure, package, justify, and defend the institution continue expanding around them.

Modern technology procurement increasingly amplifies this problem.

Cloud infrastructure, cybersecurity frameworks, insurance requirements, recurring licensing models, vendor ecosystems, outsourced monitoring, and compliance language now create environments that many smaller institutions struggle to navigate independently.

This is particularly true in municipalities and small organizations where leadership may be highly capable operationally yet lack deeply embedded senior technical guidance directly tied to mission requirements.

In those environments, organizations often gravitate toward the safest defensible procurement decision rather than the most operationally proportional one.

That distinction can become extraordinarily expensive over time.

A small town may spend enough money on outsourced technology systems to fund additional police officers — yet almost nobody can clearly explain where the money went.

Not because cybersecurity is unimportant. Modern threats are real. Police departments cannot ignore ransomware attacks, CJIS requirements, or data protection obligations.

But taxpayers should still be able to understand what they are buying.

Instead, many organizations now operate inside systems so layered and complicated that even experienced people struggle to separate:
labor,
licensing,
cloud hosting,
security tooling,
monitoring systems,
consulting fees,
vendor management,
and recurring operational overhead.

The bills continue growing while accountability becomes harder to identify.

Nobody intentionally designed it this way.

Most of the time the drift happens gradually and with good intentions.

One more security layer.
One more subscription.
One more reporting platform.
One more vendor.
One more dashboard.
One more compliance review.

Eventually the system becomes so complicated that ordinary people — and sometimes even leadership itself — can no longer clearly explain the total operational picture.

That is when budget discipline begins slipping away.

Over the last several years, CIO discussions across both government and private industry have increasingly shifted away from simplistic “cloud-first” thinking toward more nuanced hybrid strategies based on workload placement, resiliency, operational requirements, and long-term cost visibility. Industry reporting increasingly describes “cloud-smart” approaches where organizations reassess which workloads truly belong in cloud environments and which may operate more efficiently under direct operational control.

At the same time, public reporting has documented organizations reconsidering aggressive cloud-first strategies after discovering that recurring operational expenditures expanded far beyond original expectations.

Concerns now regularly include:
vendor lock-in,
recurring SaaS growth,
cloud egress fees,
expanding security tooling,
migration reversal costs,
and recurring licensing structures that become extraordinarily expensive to unwind once dependency structures are deeply embedded.

This has contributed to growing discussions around “cloud repatriation” — bringing portions of infrastructure and operational control back under direct management.

This does not mean cloud systems are bad.

Cloud computing can provide extraordinary resiliency, geographic redundancy, disaster recovery, and scalability when deployed intentionally and proportionally.

The issue is not cloud computing itself.

The issue is whether leadership fully understands the long-term operational and financial tradeoffs before dependency structures become deeply embedded.

The same pattern increasingly appears throughout healthcare.

I work with highly respected pediatricians who spent decades building independent medical practices focused on patient care and community trust. Several eventually sold their practices to larger healthcare organizations such as Advocare — not because they suddenly lost the ability to practice medicine, but because the surrounding operational systems became extraordinarily difficult to manage independently.

Insurance systems increasingly required administrative escalation, appeals processes, coding oversight, prior authorization management, legal review, and staffing structures larger organizations could absorb more efficiently through scale.

Human resources requirements expanded dramatically.

Then there was technology:
electronic medical records,
cybersecurity compliance,
insurance security expectations,
endpoint protection,
vendor management,
cloud systems,
outsourced IT governance,
and recurring licensing.

Eventually many physicians reached a difficult conclusion:

they could either continue practicing medicine or continue managing the increasingly burdensome operational machine surrounding medicine.

So independent practices consolidated into larger organizations better equipped to absorb the administrative weight.

The irony is that many systems introduced to improve efficiency ultimately contribute to rising healthcare costs for everyone else.

The same dynamic appears in municipal government.

One of the least understood realities in technology environments is that not every system requires the same security posture.

A local systems administrator supporting a police department may maintain Windows infrastructure, backups, workstation support, internet connectivity, and operational uptime.

That does not necessarily mean the administrator possesses investigative access to sensitive law-enforcement records themselves.

Systems like CODY Systems maintain their own operational credentialing and access structures.

The same separation exists throughout healthcare environments. An IT administrator may manage Active Directory infrastructure, backups, and workstation environments without possessing operational access to protected patient medical records.

The military has long understood this principle.

During my years in the Marine Corps working around aviation supply computer systems, distinctions between operational environments mattered enormously. The Department of Defense maintains separate operational assumptions for systems like NIPRNet and SIPRNet because different environments require different mission requirements, operational controls, and security models.

Not every system requires the same level of restriction.

But once compliance language, vendor marketing, procurement fear, insurance pressure, and institutional anxiety begin blending together, organizations can start purchasing generalized reassurance instead of carefully scoped operational security appropriate to the actual mission.

That distinction can become extraordinarily expensive.

And once major institutional decisions are made, another dynamic often appears.

Nobody wants to admit the system may have become too large, too expensive, or too complicated.

At that point institutional self-protection quietly begins competing against honest reassessment.

Public officials do not want to appear irresponsible.
Vendors do not want contracts questioned.
Consultants do not want recommendations reversed.
Boards do not want to explain escalating costs.
Leadership teams do not want to appear technically uninformed after publicly supporting modernization efforts.

So systems continue expanding.

The public sees rising expenditures while operational clarity continues shrinking.

Eventually citizens begin asking uncomfortable questions.

Why are costs still rising?

Why does every solution require another subscription?

Why are staffing shortages growing while administrative overhead expands?

Why does nobody seem fully accountable?

These questions become especially dangerous when operational failures begin appearing publicly.

The aerospace industry learned this lesson painfully.

Investigations surrounding the Boeing 737 MAX disasters raised serious questions about the relationship between engineering concerns, certification oversight, production pressure, and corporate decision-making. Congressional hearings, FAA investigations, and public reporting documented concerns involving MCAS flight-control assumptions, internal warning signals, pilot training decisions, and organizational pressure tied to schedule and market competition.

The issue was not simply technical failure.

The issue was whether organizational systems remained sufficiently connected to engineering judgment and operational reality.

Several hundred lives were lost before the abstraction collapsed under the weight of reality.

The lesson extends far beyond aviation.

Modern warfare is teaching similar lessons in real time.

The war in Ukraine has demonstrated how rapidly smaller operational groups can innovate around low-cost drone systems and battlefield adaptation while larger procurement systems struggle with layered acquisition structures and slower operational responsiveness.

Again, the lesson is not that large institutions are unnecessary.

The lesson is that systems become fragile when presentation overtakes truth, process overtakes mission, and abstraction overtakes accountability.

Not long ago, I attended a meeting at a church in Elkton concerning a relatively straightforward website update. The technical work itself was manageable and the meeting should have ended quickly.

But after the official discussion ended, the pastor and a high-school math teacher serving on the church board kept the conversation going.

They asked a harder question.

What could actually help young people struggling in town?

My answer had nothing to do with technology.

I suggested programs that provide structure, mentorship, accountability, leadership, and practical skill development — things like scouting, athletics, apprenticeship, JROTC, and hands-on mentorship.

Not because those programs are perfect.

But because they require something modern institutions increasingly struggle to provide:

real human investment.

Someone has to show up.
Someone has to mentor.
Someone has to teach.
Someone has to care.

That problem cannot be outsourced to software, dashboards, consultants, or compliance systems.

Communities do not become stronger through institutional theater alone.

Healthy institutions still depend upon trusted people carrying real responsibility.

That is true in policing.
It is true in medicine.
It is true in engineering.
It is true in military leadership.
And it is true in local government.

The danger facing modern institutions is not technology itself.

The danger is slowly drifting into systems where nobody fully understands the costs, nobody clearly owns accountability, and polished institutional theater begins replacing operational truth.

This is not an argument against business, cybersecurity, modernization, or accountability.

Those things matter.

It is an argument for balance.

Taxpayers deserve understandable budgets and visible accountability.

Police chiefs deserve systems that support officers rather than bury them under unnecessary complexity.

Doctors deserve systems focused primarily on patient care.

Engineers deserve environments where operational truth matters more than presentation.

And communities deserve institutions connected to reality instead of institutions increasingly consumed by process, abstraction, and performance theater.

The solution is not revolution.

The solution is leadership willing to ask uncomfortable but necessary questions.

Are we solving real problems — or buying reassurance?

Are we helping the people doing the work or burying them?

Are we strengthening resilience or simply expanding bureaucracy?

Most importantly:

Are our systems still serving the mission — or are we slowly serving the systems themselves?

— Jim Hansen
Founder, Hi5s, Inc.
Bear, Delaware