2 Stories Collection

2.1 Story: ArcoMed cloud-first

ArcoMed is a regional public health provider in southern Europe, managing several hospitals and health centres. Two years ago, its leadership embraced a cloud-first strategy, aligned with national digital health ambitions. The CIO, politically well-connected, secured fast-track approval to migrate critical systems — including electronic health records and imaging platforms — to an external vendor's cloud infrastructure.

The project was applauded as visionary, but governance was shallow. No Data Protection Impact Assessment (DPIA) was performed, and procurement decisions bypassed formal consultation with clinical or operational leads. Internal staff described the initiative as "done to us, not with us." Though the system initially improved access and reporting, responsibility for local resilience was unclear — internal IT believed the vendor handled backup; the vendor insisted local fallback was ArcoMed's job.

Then came the crisis: a targeted cyberattack disrupted the vendor's cloud platform. For over 36 hours, all clinical systems were inaccessible. Staff had to scramble to find incomplete paper backups. Elective surgeries were cancelled. News outlets framed it as a digital governance failure.

The CIO publicly blamed the vendor, citing the service-level agreement (SLA). The vendor countered that key risk mitigation steps — including local restoration mechanisms — were never implemented by ArcoMed's internal IT. The Chief Medical Officer, blindsided by the extent of the disruption, criticised the lack of shared planning. Union representatives called the episode "a consequence of managerial opacity."

Now, the Board has requested an independent review of governance maturity, project accountability, and the internal management system that allowed such blind spots. Political pressure is mounting for increased transparency and for clearer roles in digital transformation oversight.

2.2 Story: ArcoMed cloud migration

ArcoMed, a regional public health provider, launched a flagship cloud migration initiative, moving its electronic health records and imaging systems to an external provider's cloud platform. The project, led by the CIO and supported by national digital health agendas, aimed at rapid innovation and increased efficiency.

However, the initiative lacked a structured governance of IT framework. No DPIA (Data Protection Impact Assessment) was performed. Strategic oversight of IT risk, vendor accountability, and fallback mechanisms remained unclear. While the CIO held operational power, no decision-rights matrix or formal alignment mechanisms ensured coherence between business governance and IT governance structures.

When a cyberattack disabled the cloud infrastructure, clinical operations collapsed for over 36 hours. Internal IT teams lacked fallback access, and vendors denied responsibility for local recovery. Clinical leadership had not been involved in the planning or testing of resilience protocols.

After the event, a governance review revealed a weak separation of strategic and operational concerns, absence of formal role mapping (e.g., no RACI structure), and immaturity in the institution's governance of IT posture. The Board and the regional health authority now face scrutiny for not ensuring the CIO's initiatives were framed within robust, institution-wide IT governance practices — including vendor risk management, system criticality mapping, and compliance traceability.

2.3 Story: ArcoMed ransomware

ArcoMed, a regional public health provider, had transitioned key hospital systems — including electronic records and imaging services — to a third-party cloud platform. The shift promised agility and lower maintenance, but internal IT operations were insufficiently restructured to cope with the new architecture.

Operational readiness was minimal: local backups were outdated, service restoration protocols were undocumented, and disaster recovery procedures were never tested. Monitoring and alerting tools were fragmented. No incident response playbook linked operational roles across clinical and IT teams.

When the cloud vendor suffered a ransomware attack, all services were lost for over 36 hours. Staff attempted to recover from scattered, incomplete backups. Elective surgeries were postponed. Communications between IT operations and hospital units broke down.

The vendor pointed to standard SLA clauses and disclaimed responsibility for local contingency measures. Internal IT staff, caught between unclear escalation paths and absent fallback infrastructure, were unprepared to mitigate the crisis.

Post-crisis audits exposed serious flaws in ArcoMed's IT service management (ITSM) practices: no change management log, outdated configuration documentation, and no formalised operational risk registry. Leadership demanded a complete overhaul of IT operations, including adoption of incident management frameworks (e.g., ITIL), and sector-appropriate resilience protocols.

2.4 Story: VisioRetail AI Misfire

When the CEO of **VisioRetail**, a mid-sized European chain of home goods stores, declared that the company would become "AI-driven by design," it caught the attention of both the press and investors. The announcement followed a costly pandemic-era dip in performance and was part of a turnaround strategy led by an ambitious CTO, Carolina Riva, recently poached from a Silicon Valley startup.

Carolina had strong technical credentials and a bold plan: to integrate machine learning models for demand forecasting, optimise supply chain logistics, and implement a generative AI-powered chatbot to replace most human customer service. She insisted on agile implementation and hired a boutique AI consultancy with no retail background but a flashy demo. The CIO, an internal veteran named Nuno Esteves, raised concerns about legacy system compatibility, but was sidelined early in the project.

One year in, results were mixed. The chatbot struggled with multilingual support and failed to handle refunds correctly. The AI forecasts ignored weather effects and local holidays, resulting in bizarre stock allocations. Warehouse efficiency actually declined due to over-reliance on automated triggers that bypassed human intuition.

Meanwhile, staff morale plummeted. Shop floor workers felt alienated by the rapid changes, and regional managers complained of being turned into "button-pushers." Customers began posting stories online about poor service and surreal AI replies. By the time the board demanded an internal audit, it was clear the transformation had prioritised technological ambition over operational alignment and stakeholder engagement.

In the post-mortem, it became evident that no strategic portfolio review had been conducted. There was no Target Operating Model (TOM), no alignment between IT capabilities and business processes, and no stakeholder mapping. The CTO resigned. The CIO was called back in to lead a more inclusive, phased realignment effort—starting with defining what "AI-driven" should mean in a retail business context.

2.5 Story: VisioRetail CEO Shuffle

VisioRetail, a fast-expanding home and lifestyle retail chain in Southern Europe, was known for its daring digital bets. But beneath the shiny innovation, board-level tensions were simmering.

The previous CEO, Raul Andrade, had led the company through aggressive expansion, heavily investing in automation and predictive analytics. While this earned media praise, internal governance was weak. Raul maintained tight executive control and bypassed traditional reporting channels, relying instead on a small "strategy cell" reporting directly to him. The board, impressed by growth numbers, remained passive.

In Q2 2024, sales plummeted in several regions, and a whistleblower flagged undisclosed losses due to mismanaged stock and overpromised supplier contracts. As pressure mounted, the board forced Raul to resign and appointed an interim CEO, Sofia Matos, previously Head of Compliance. Her mandate: restore governance maturity and rebuild internal trust.

Sofia quickly discovered the absence of a functioning management system: KPIs were inconsistent across departments, risk registers were outdated, and accountability was blurred. There was no audit trail on critical IT contracts. While the CIO had been technically competent, he had no board-level access and had been routinely sidelined from strategic discussions. The HR director had resigned a year earlier, citing "values drift."

Sofia restructured the executive team and initiated a governance review based on the ISO 37301 framework. She invited staff into stakeholder sessions and brought in an external auditor to rebuild control functions. The board, now more aware of its oversight role, established a formal risk committee and mandated annual reviews of the management system.

As the company entered its next strategic cycle, Sofia raised an internal discussion: was VisioRetail's culture too enamoured with charismatic leadership? And could sustainable governance take root in an organisation built on speed and intuition?

2.6 Story: MetroWater Access Denied

MetroWater is a large public utility responsible for water distribution and wastewater management in a densely populated metropolitan region. As part of a national push for smart infrastructure, MetroWater launched an ambitious programme to digitise field operations, introduce predictive maintenance, and consolidate SCADA (Supervisory Control and Data Acquisition) systems into a unified cloud-enabled platform.

The CIO championed the effort, outsourcing both the systems integration and platform management to a multinational vendor. The contract was signed under pressure to comply with tight national funding deadlines, and key technical staff were excluded from final design reviews.

Soon after deployment, technicians began reporting erratic remote access to pump stations. Field operators could no longer override sensors on-site when cloud access failed. A routine firmware update caused a cascading failure that blocked control of three major stations for 12 hours. Water pressure dropped city-wide. Emergency protocols had to be triggered manually by staff unfamiliar with the digital failover procedures.

An internal review exposed systemic gaps: no operational continuity testing, unclear responsibilities for patch approval, and lack of alignment between MetroWater's risk management framework and the vendor's change control process. Documentation was fragmented across systems. The CIO insisted the vendor was responsible, while the vendor pointed to MetroWater's lack of role definitions and fallback plans.

Under scrutiny from the municipal oversight committee, MetroWater admitted there was no IT governance model linking critical infrastructure oversight with vendor service levels. There were also no metrics in place to track resilience or recovery capacity. A whistleblower claimed internal warnings had been ignored because "governance was treated as a compliance checkbox, not an operational necessity."

2.7 Story: MetroWater Leap Too Far

MetroWater, a large urban utility responsible for water and wastewater services, faced increasing political pressure to modernise its image and services. In response, the new CEO launched a high-profile strategic transformation programme titled *"MetroWater 4.0"*, aiming to position the organisation as a smart utility leader through automation, digital customer engagement, and AI-based consumption analytics.

The initiative was led by a freshly appointed Chief Strategy Officer, who came from the energy sector. The CIO and the Operations Director were only consulted at the implementation stage. No enterprise architecture modelling or Target Operating Model was developed. Business process owners were instructed to adopt pre-packaged "innovation accelerators" offered by the vendor without adaptation.

Internally, employees struggled to understand how their work fit the new tools. Billing support agents were suddenly asked to interpret machine-generated risk scores. Customer complaints surged when billing algorithms applied penalties based on faulty assumptions. Union representatives protested the speed of automation and accused leadership of "consultant-led chaos."

The board was unaware that the transformation lacked integrated KPIs or formal strategic portfolio governance. The CEO had delegated decision-making to the CSO, who focused on short-term deliverables over cross-departmental coordination. When the first quarterly review showed reputational damage and cost overruns, a governance crisis emerged.

An internal audit found the management system was not updated to reflect the transformation programme. Department heads reported "vision without structure." The CIO later noted that digital ambitions had outpaced both operational capacity and managerial clarity, with no coherent roadmap to ensure long-term alignment.

2.8 Story: BeaconLab Algorithmic Secret

BeaconLab is a private biotech start-up owned by John José and known for rapid development of diagnostic software using machine learning. In 2024, it launched an internal challenge to compress DNA sequence analysis into a mobile application that could deliver results in under 10 seconds. A team of junior data scientists announced that they had succeeded by creating a new custom algorithm optimised for GPU acceleration.

The app was celebrated internally and posted as a preprint on a public research server. However, a few weeks later, John José discovered that the algorithm violated a clause in a third-party academic code licence. The developers' team had copy-pasted parts of the original algorithm without proper attribution, believing that code snippets published in public forums were "community-owned."

BeaconLab apologised and voluntarily took the app offline. A disciplinary review led to temporary suspension of two developers. John José issued a statement reaffirming the company's commitment to scientific ethics.

Following the incident, BeaconLab adopted a mandatory open-source compliance checklist for developers and hired a legal advisor. The company resumed operations, and the preprint was withdrawn. Some of the affected researchers later joined a university spin-off.

2.9 Story: BeaconLab Growth Pains

BeaconLab, a rapidly scaling biotech company, earned global attention for its AI-based diagnostics and mobile DNA testing platform. Flush with investor funding, the leadership launched a growth initiative to accelerate time-to-market for new algorithmic services by shifting from research-based software governance to an industrial-grade cloud architecture.

The CTO partnered with a digital consultancy to implement a new cloud-native analytics pipeline but skipped formal architectural reviews to maintain momentum. Internal documentation was scattered, and developer teams were left to self-organise code management using public repositories. An internal DevOps team raised concerns about lack of secure API governance and licensing controls, but their feedback was not escalated.

A month before launch, BeaconLab received a legal notice from a university claiming their core sequence compression engine violated terms of a research licence. An audit confirmed that one of the algorithm components had been used without proper integration review or reuse authorisation. The CTO had assumed the open code fell under "fair experimental reuse," but no due diligence process was in place.

To contain reputational fallout, the product launch was delayed. The CEO initiated a strategic realignment, mandating governance for code reuse and open-source dependencies. A new Enterprise Architecture team was created to oversee component integration, and a board-level risk committee was formed to align research agility with commercial compliance requirements.

BeaconLab now applies a dual-track innovation framework: one focused on exploratory research, and another governed by structured production and risk management processes. Developers attend onboarding sessions on IP risk, and all product modules undergo alignment review between IT, legal, and business units.