



ANATOMY OF A FAILED TRANSFORMATION: THE BRITISH AIRWAYS OPERATIONAL COLLAPSE

British Airways' IT meltdown in May 2017 is the definitive case study in operational transformation risk. Over a bank holiday weekend, a power failure at the airline's primary data centre grounded all flights at Heathrow and Gatwick, stranding 75,000 passengers and costing the parent company £80 million in compensation and lost revenue.

This wasn't a slow-motion budget blowout like CBA, a strategic drift like GovERP or a migration disaster like TSB. It was an immediate, total **operational collapse** caused by a single maintenance error and the complete **absence of resilience to recover** from it.

The root cause: an engineer powered down a major data centre's uninterruptible power supply (UPS) without proper authorisation or oversight. The cascading power failure damaged core systems, and it took days to manually restart operations because automated failover procedures either didn't exist or didn't work.

The Fatal Flaw: Process Without Operational Discipline

While BA had been undergoing cost-cutting and transformation initiatives, the failure exposed fundamental weaknesses in People and Process that left critical infrastructure vulnerable to human error.

The regulators and investigators identified three structural failures:

- **Single point of failure in process:** The incident was triggered by a contractor overriding system controls during routine maintenance. There was no robust process governance for critical infrastructure work no checks, no approvals, no monitoring.
- **Failure of people and training:** The engineer involved reportedly lacked proper training and certification for the work being performed. BA had over-relied on poorly supervised contractors for critical infrastructure, creating a fatal gap in operational capability.
- **Lack of resilience and recovery:** When the power failed, automated failover systems didn't work. Recovery mechanisms that should have kicked in automatically either didn't exist or were insufficient for the scale of the physical shutdown. Manual restart took days instead of hours. This case proves that cost-cutting in operations and training isn't efficiency it's investing directly in operational risk.



The Leader's Mandate: Governing Critical Infrastructure

The BA collapse demonstrates that operational transformation requires treating your data centre and core infrastructure as critical business assets that need active governance, not static utilities that just need to be kept running cheaply.

This is the non-negotiable governance required for operational resilience:

1. Test Your Failure Scenarios

Establish regular simulation and audit of catastrophic failure scenarios full power-downs, human error in maintenance, failed patches. Testing must include the actual people who would respond to the crisis, not just technical documentation that assumes everything works. If you can't prove your systems recover from failure, you don't have resilience.

2. Govern Maintenance as Transformation Risk

Any maintenance or change in Tier 1 infrastructure regardless of whether it's performed by internal staff or contractors must follow standardised, auditable change management protocols. BA's failure resulted from a process gap where critical work happened without proper oversight. These protocols must be monitored at executive risk management level, not buried in IT operations.

3. Invest in Capability, Not Just Capacity

All individuals with access to critical infrastructure controls must undergo annual, independently verified certification tied to performance reviews. Stop treating outsourcing as pure cost-saving it's an accountability transfer that requires rigorous management through SLAs and mandatory training standards. If contractors can take down your business, you need to know they're qualified to touch it.

Strategic Conclusion

The BA meltdown serves as a harsh reminder in the digital age, your operational infrastructure is your entire business. A single error by a single person can stop global operations.

The airline industry is unforgiving, planes either fly or they don't, customers either get to their destination or they're stranded. But every industry now has the same operational exposure. Your core systems are either resilient enough to survive human error and infrastructure failure, or they're not. If your infrastructure is undergoing transformation or cost optimisation, ask yourself: **Are you testing for resilience, or just assuming it exists?**

This is the challenge Telos Program Partners solves. We embed the operational governance and resilience testing needed to ensure your core systems can survive real-world failures not just function when everything goes according to plan. When operational continuity defines your business, we ensure your infrastructure and processes are genuinely resilient.

Contact: maria@telosprogrampartners.com.au | +61 431 503 456 | www.linkedin.com/in/mariahantes

Sources: IAG Annual Reports (2017); BA Public Statements; UK CAA Investigation Reports; Financial Press Analysis.