

Operational Resilience For IT Leaders: Key Priorities for 2026

Sustaining cyber resilience goes beyond meeting compliance requirements. IT leaders must continuously monitor controls, ensure operational effectiveness, and respond proactively as environments evolve.

This snapshot highlights the critical areas to oversee and act on in 2026, helping you safeguard operations and demonstrate strategic value to the business.

KEY OPERATIONAL FOCUS AREAS

- **Patch Management:** Ensure timely deployment across all applications and operating systems to reduce exploitable vulnerabilities.
- **Access & Privileges:** Regularly review accounts, restrict admin rights, and enforce MFA to minimise insider and external risks.
- **User Hardening:** Maintain secure configurations for productivity tools and browsers to prevent compromise.
- **Backup & Recovery:** Verify schedules, storage integrity, and restoration processes to guarantee rapid recovery from incidents.

RESILIENCE METRICS TO TRACK

Monitor and review these metrics to measure resilience performance and drive informed IT decisions:

- **% of systems with fully applied controls:** Monitor completeness and identify gaps.
- **Frequency of control validation and remediation:** Ensure continuous operational effectiveness.
- **Mean Time to Recover (MTTR) from incidents:** Assess real-world resilience.
- **Coverage of high-risk systems under continuous monitoring:** Prioritise resources where they matter most.

CONNECTING IT PERFORMANCE TO BUSINESS OUTCOMES

- **Translate metrics into business impact:** Present dashboards that clearly show how IT performance affects operational continuity.
- **Highlight critical risks:** Link technical issues to potential disruptions in business processes.
- **Demonstrate strategic value:** Showcase how IT initiatives strengthen organisational resilience and support key business objectives

By focusing on these operational priorities and tracking the right metrics, IT leaders can maintain resilient systems, reduce risk, and demonstrate the strategic value of IT to the broader organisation.

Use this snapshot as a reference to guide decisions, allocate resources effectively, and ensure your organisation is prepared to respond quickly to evolving threats in 2026.