ITSM Work Samples & Case Studies

Three hypothetical scenarios | Public-safe portfolio sample

Case 1 — Critical Application Outage

A business-critical application becomes unavailable for a broad user group. Response approach: • Assess business impact and severity using approved criteria.
• Establish incident command, roles and technical workstreams.
• Communicate confirmed facts, actions, owners and next update.
• Validate recovery technically and with business users.
• Review detection, dependencies, recovery readiness and action effectiveness.

Case 2 — Access-Control Mismatch

A routine onboarding or configuration activity results in permissions inconsistent with the approved access model. Response approach: • Assess exposure and contain through approved procedures.
• Identify affected accounts/scope and engage security as required.
• Correct access and validate least-privilege outcome.
• Review role mapping, approvals and post-change checks.
• Track control improvements and effectiveness evidence.

Case 3 — Degradation After Planned Maintenance

Intermittent service failures appear after a scheduled maintenance window. Response approach: • Link incident and change records; review implementation evidence.
• Assess dependencies, rollback and forward-fix options.
• Coordinate technical actions and business-impact updates.
• Validate service stability and recovery.
• Improve change assurance, dependency checks and early-life support.

All case studies are hypothetical and do not represent actual employer or customer incidents.