

Mang Morgan

ASSURANCE

ISO/IEC 27001:2022

Internal audit report Selected results

Northstar Sports Club Limited

Representative fictional sample - not a historical client engagement.

A simulated SaaS engagement demonstrating our documentation approach. All organisations, records, observations and results are fictional. No audit, interview, test or professional sign-off was performed.

Document	MMA-PUB-RPT-001 Public demonstration extract v1.0
Legal provider	Mang Morgan Capital Limited, trading as Mang Morgan Assurance
Document owner	Nimbe Akerele, CISA
Issue / classification	11 October 2026 Public fictional demonstration
Scenario fieldwork	14-18 September 2026 Remote Five days
Scenario report cutoff	18 September 2026 at 17:00 UTC; report dated 25 September 2026
Basis	Original authored scenario v2.0; standards references and original summaries only

This extract is not a certification-readiness opinion, real client report, full audit methodology or substitute for licensed standards. The complete working pack is kept separately for a guided scoping discussion.

Scope, criteria and method

Scope	The design, development, operation and support of the Northstar sports-management SaaS platform and supporting corporate functions delivered by Northstar Sports Club Limited from Ireland.
Locations	Dublin, Ireland - fictional registered office; Remote workforce - Ireland and United Kingdom
Systems	AWS production environment; Microsoft 365 corporate environment
Activities	SaaS product development; Cloud operations; Customer support; Supplier management; Corporate governance
Operating period	1 June-18 September 2026, with historical supplier due dates and May vulnerability detections included to test continuing obligations.
Criteria	ISO/IEC 27001:2022 including Amendment 1:2024; fictional SoA v2.3; original scenario policies. No copyrighted requirement text reproduced.

How the scenario is assessed

The authored exercise follows agreed scope, document review, interviews, risk-based selection, control tests, evidence evaluation and reporting. The five-day plan is distinct from planning, analysis, report writing and review time.

Supplier sampling deliberately selects all three critical suppliers from 18 active suppliers. Vulnerability sampling selects three high-severity records from a 12-record July cohort, including both overdue items. These purposeful selections are not statistical prevalence estimates.

Objectivity in the scenario

The fictional acceptance record states no prior implementation/advisory involvement, financial benefit or management responsibility. Read-only access and client ownership of risk decisions are planned safeguards. No actual independence declaration or reviewer signature is claimed.

Executive summary

The scenario demonstrates how operating controls and exceptions are reported together. Authored examples show approved access grants, release approvals and recovery against defined objectives. Two selected failures are recorded as minor nonconformities and one presentation improvement as an OFI.

Classification	Unique findings in this scenario
Major nonconformity	0
Minor nonconformity	2
Opportunity for improvement	1

These counts describe findings, not the percentage of controls compliant or a certification-readiness score.

NSC-NC-01 | Minor nonconformity

Critical supplier monitoring decision overdue without approved deferral

Related workpaper: NSC-WP-13 | Reference: A.5.22

NSC-NC-02 | Minor nonconformity

Overdue high vulnerability lacks approved exception decision

Related workpaper: NSC-WP-21 | Reference: A.8.8

NSC-OFI-01 | Opportunity for improvement

Consolidate management targets, trends and owners for easier evaluation

Related workpaper: NSC-WP-04 | Reference: 9.1

Coverage

The full authored pack contains 25 process workpapers, 30 clause-index rows and all 93 Annex A control references. A process may support several references. Indexing does not prove exhaustive normative coverage, identical testing or conformity of every transaction. This public extract contains selected results only.

Conclusion and limitations

The authored results support an established and operating ISMS within the selected boundaries: access approvals precede grants, sampled releases retain independent approval and tested rollback, recovery meets the 4-hour/24-hour objectives, and monthly analysis identifies and escalates exceptions. They do not support unqualified conformity: SUP-014 lacks its due monitoring decision/deferral and VUL-077 exceeds the adopted remediation deadline without prior approval. These two minor nonconformities remain Open at the 25 September initial report; optional consolidation of already-defined performance information is one OFI. The 30 clause and 93 applicable-control evaluations support scope coverage, not a compliance score or evidence of every transaction. Bounded judgmental selections, remote physical demonstrations, indirect provider evidence and no-occurrence exercises limit assurance; sustained effectiveness or certification readiness is not concluded. No real fieldwork or conformity opinion is represented.

What the classifications mean

Conforming	The examined evidence supports the agreed requirement within the stated sample and limits.
Major nonconformity	A failure with significant effect on the system's ability to achieve intended outcomes; used only where the agreed methodology permits.
Minor nonconformity	A requirement is not met, without the demonstrated extent/impact supporting a major classification. This is not a low-risk rating.
Opportunity for improvement	No requirement failure is established; an optional improvement may be considered.

Management and follow-up

The audited organisation owns root-cause analysis, correction, corrective action and implementation. Both nonconformities remain Open at the initial scenario report date. Subsequent verification is a separate activity and does not rewrite the initial result.

No real fieldwork, security testing, authenticity verification, sustained effectiveness conclusion or certification decision is represented. Physical/provider assurance is indirect and remote; the scenario has bounded, judgmental samples.