

Mang Morgan

ASSURANCE

ISO/IEC 27001:2022

Findings register

Selected findings

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-FND-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.

NSC-NC-01 | Minor nonconformity

Critical supplier monitoring decision overdue without approved deferral

Reference	A.5.22
Workpaper / test	NSC-WP-13 NSC-WP-13-S04
Initial status	Open
Scenario report date	2026-09-25

Requirement / assessment criterion

NSC-SUP-POL-002 v2.1 section 5.2: Critical suppliers need a monitoring decision every 12 months; a deferral requires COO approval, revised date and rationale before the due date; Procurement retains the decision/deferral.

Objective evidence - authored scenario

18 active suppliers; critical SUP-002/SUP-009/SUP-014 selected. SUP-014 has a 18 December 2024 decision and 18 December 2025 due date, but no retained 2025 monitoring decision or approved deferral at fieldwork. Contracts and initial due diligence exist.

Conformity gap

The agreed monitoring cycle was not evidenced or formally deferred for SUP-014.

Classification rationale

All 3 Critical suppliers were examined (3 of 18 total), and an all-18 due-date extent screen identified only SUP-014 overdue. The 272-day delay at 16 September spans one missed annual cycle, not multiple missed anniversaries. Contract/delivery safeguards and the other two monitoring decisions remain in operation. The documented handover failure is bounded but requires systemic ownership/escalation correction. These authored facts support minor classification, not low business risk or proof of no supplier compromise.

Management owns any response and implementation. An OFI does not require a corrective-action response. All records here are fictional; no audit or actual sign-off was performed.

NSC-NC-02 | Minor nonconformity

Overdue high vulnerability lacks approved exception decision

Reference	A.8.8
Workpaper / test	NSC-WP-21 NSC-WP-21-S01
Initial status	Open
Scenario report date	2026-09-25

Requirement / assessment criterion

NSC-VM-POL-001 v1.4 section 4.3: High findings have a 30-calendar-day target; before deadline an extension requires Security/Compliance Manager approval, named risk owner, rationale, compensating safeguards and revised date retained in the exception register. Engineering notes are not approval.

Objective evidence - authored scenario

31 July export includes two high overdue items. VUL-072 detected 10 May/due 9 June has EX-072 approved 7 June by Sofia with Ava risk owner and 30 September revised date. VUL-077 detected 25 May/due 24 June is 67 days old at 31 July and 114 days old at 16 September; it lacks approved exception/revised date in both snapshots. Engineering dependency notes are not authorisation. VUL-081 detected 25 June was remediated/clean-rescanned 14 July (19 days).

Conformity gap

The vulnerability exception process was not applied to one overdue high-severity item.

Classification rationale

The 12-record cohort extent screen includes all 3 High items; only VUL-077 has an unauthorised extension. The affected restricted nonproduction test runner has no direct internet ingress or customer data; scanner/triage/remediation and an approved comparator operate. These bounded facts support minor classification despite prolonged delay. No observed exploit signal is not proof of no exploitation; risk priority remains elevated and no claim covers vulnerabilities outside the cohort.

Management owns any response and implementation. An OFI does not require a corrective-action response. All records here are fictional; no audit or actual sign-off was performed.

NSC-OFI-01 | Opportunity for improvement

Consolidate management targets, trends and owners for easier evaluation

Reference	9.1
Workpaper / test	NSC-WP-04 NSC-WP-04-S02
Initial status	Open - optional management consideration
Scenario report date	2026-09-25

Requirement / assessment criterion

Monthly measures retain source, calculation, target and management review decision; no consolidated dashboard design is mandated.

Objective evidence - authored scenario

June-August packs specify measures, methods/source calculations, monthly collection/evaluation dates and responsible owners; source counts, trend analysis and management decisions are retained and meet the defined schedule. Targets, trends and owners are in separate tabs; consolidation is optional. No gap in the defined monitoring/evaluation elements was identified.

Optional improvement

Optional presentation improvement only; no nonconformity identified.

Classification rationale

A consolidated view could reduce management evaluation effort without inventing a mandatory dashboard format.

Management owns any response and implementation. An OFI does not require a corrective-action response. All records here are fictional; no audit or actual sign-off was performed.