MAZDEN TECH

Environment Assessment — Illustrative Sample

Illustrative sample — not a customer assessment. Final findings and service targets are developed for your environment.

Prepared for: [Client / Company Name] · Prepared by: Mazden Tech · mazdentech.com · tmaddenjr3@gmail.com · Date: [Date] · Sites: [City / site list] · Users / devices: [#] / [#]

1. Systems / applications register

Lean inventory of in-scope systems. Access verification records named custodians only — no passwords, MFA codes, or secrets are collected on this worksheet. Criticality labels: Critical · Important · Standard · Convenience.

System / app	Tech admin	Business owner	Criticality	Key dependencies
[e.g. Illustrative — Identity / email]	[Name / role]	[Name / role]	[Critical]	[Identity · network · upstream]
[e.g. Illustrative — Line-of-business app]	[Name / role]	[Name / role]	[Important]	[Depends on…]
[System name]	[Name / role]	[Name / role]	[Standard / Convenience]	[Dependencies]

2. Prioritized findings

Priority	Finding	Affected systems / process	Suggested next step
P1	[Finding title]	[System / process]	[Stabilize / project / vendor]
P2	[Finding title]	[System / process]	[Stabilize / project / vendor]
P3	[Finding title]	[System / process]	[Stabilize / project / vendor]

3. Proposed severity framework

Proposed for confirmation — not active until approved in writing. Numeric targets remain [TBD / agreed]. Sev1: critical process down / no workaround or broad core outage. Sev2: material multi-user degradation with partial workaround. Sev3: limited impairment with acceptable workaround. Sev4: requests / planned changes.

Severity	Coverage hours	Ack / initial response	Update cadence	Workaround / restore	Full resolution
Sev1	[TBD / agreed]	[TBD / agreed]	[TBD / agreed]	[TBD / agreed]	[TBD / agreed]
Sev2	[TBD / agreed]	[TBD / agreed]	[TBD / agreed]	[TBD / agreed]	[TBD / agreed]
Sev3	[TBD / agreed]	[TBD / agreed]	[TBD / agreed]	[TBD / agreed]	[TBD / agreed]
Sev4	[TBD / agreed]	[TBD / agreed]	[TBD / agreed]	N/A	[TBD / agreed]

Business recovery goals — recovery time objective (RTO: how quickly a system should be usable again) and recovery point objective (RPO: how much data loss is acceptable) — are recorded separately from provider response commitments. Security incidents follow an agreed incident-response path. Third-party restore outcomes depend on the upstream vendor.

4. Suggested next steps

1) Review register, findings, and proposed severity definitions. 2) Agree numeric targets and coverage hours in writing (or defer). 3) Confirm onboarding: inventory → access verification → stabilize → ongoing scope. 4) Proceed to Managed IT terms only after mutual approval.

Assessment scope and fee are agreed before work starts. The Calendly consultation is introductory and does not purchase an assessment. Contact: tmaddenjr3@gmail.com · https://calendly.com/tmaddenjr3/mazden-tech-consultation · https://mazdentech.com