

BunyanMatrix | Portfolio Demonstration

Fictional Microsoft 365 Security Assessment

Sample customer: Northstar Fieldworks Ltd. | 50 employees | Demonstration only | All findings and values are invented.

Purpose

This sample illustrates the approach and deliverables of a fixed-scope Microsoft 365 security baseline assessment. It is NOT a case study of a real customer, a completed client engagement, or evidence that any company experienced these weaknesses.

Hypothetical environment

Profile	Fictional baseline
Organization	50 users; cross-border consulting and project delivery
Platforms	Microsoft 365, Entra ID, Exchange Online, Teams, SharePoint, OneDrive
Assessment approach	Read-only inventory, policy inspection, evidence traceability and prioritized remediation
Demonstration scope	Identity, app consent, mail protection, external sharing, meeting controls

Sample executive finding

The fictional company has five simulated control gaps. Two are rated High, three Medium. In an actual engagement, risk ratings would be calibrated against business context and verified technical evidence.

Simulated risk register

F-001 | High | Anonymous external sharing

Simulated observation: Fictional tenant default: Anyone links; edit permitted; no expiry.

Suggested remediation: Change to Specific people and View, disable anonymous editing, review links.

F-002 | High | Privileged account without MFA

Simulated observation: Simulated IT admin uses password-only authentication.

Suggested remediation: Register phishing-resistant MFA; implement supported enforceable MFA policy.

F-003 | Medium | Excessive guest access

Simulated observation: 15 guest users, 6 inactive for more than 90 days in synthetic data.

Suggested remediation: Set ownership and periodic access reviews; remove unneeded access after approval.

F-004 | Medium | Unrestricted application consent

Simulated observation: Users may approve third-party apps with broad scopes in simulation.

Suggested remediation: Require admin approval for risky scopes and inventory existing grants.

F-005 | Medium | Teams anonymous presenter rights

Simulated observation: Synthetic meeting policy permits anyone to present by default.

Suggested remediation: Restrict default presenter role and maintain lobby checks.

Example engagement deliverables

1. Executive summary with priorities; 2. Evidence-backed configuration register; 3. Risk and action tracker; 4. Practical remediation instructions; 5. Optional verification after customer-approved changes.

Sample workflow

Discovery and authorization -> read-only review -> validation of observations -> risk prioritization -> customer presentation -> approved remediation by separately agreed scope.

Public-use disclaimer

All organization names, configurations, quantities, findings and recommendations in this demonstration are fictional. BunyanMatrix should never characterize this example as prior paid work or a real client outcome.