BITSCALED / ASSESSMENT GUIDE

Enterprise Security Overview

A practical starting point for executive, IT, and compliance leaders planning their next security assessment.

Start with your operating risk

Scope the endpoint fleet, identity platforms, compliance mandates, and threat concerns that matter to your organization. Your inquiry helps an engineer prepare a focused assessment conversation.

Identity and workspace security

Discuss privileged access, account lifecycle, multifactor authentication, and Microsoft 365 or Google Workspace configuration. Agree on the systems and access boundaries to include before assessment work begins.

Detection, resilience, and recovery

Review ransomware exposure, monitoring coverage, backup responsibilities, and recovery priorities. Define the evidence needed to evaluate gaps and prioritize remediation.

Compliance and evidence

Identify applicable HIPAA, NIST CSF, CMMC, SOC 2, or PCI-DSS requirements and the evidence your stakeholders need. Readiness support is scoped delivery work; this overview is not a certification, audit opinion, or attestation.

Choose the conversation that fits

An Async Risk Review starts with a written exchange about your priorities. A Live Architecture Briefing starts with arranging a discussion with your team. Submitting an inquiry requests a consultation; it does not reserve a meeting or authorize a security scan.

Leave with a clear next step

Confirm objectives, owners, assessment boundaries, and the information needed for a proposed scope. Any service commitments, deliverables, and pricing are agreed in the engagement terms.

Share business context only. Do not submit passwords, tokens, sensitive records, or unredacted logs. Use an agreed secure channel if an assessment later requires confidential evidence.