Violet Bridge Security LLC

Three-Pillar Service Delivery Methodology

A practitioner-led approach to cybersecurity consulting that balances strategy, visibility, and administration. This document elaborates the principles, standards, and practices underpinning our comprehensive methodology.

Pillars	Security • Visibility • Administration
Domains	Strategy & Risk • Compliance • Architecture • Data Protection • Identity • Awareness
Approach	Risk-Based • Standards-Aligned • Business-Focused

Table of Contents

1. Overview: Consulting Outcomes

Our objective is to measurably reduce business risk while enabling organizations to operate with confidence. We achieve this by aligning security strategy with business objectives, increasing true visibility over the attack surface and control effectiveness, and establishing administrative persistence—governance, ownership, and continuous improvement—that ensures improvements remain in place long-term.

The three pillars represent concurrent capabilities that are strengthened over time, not sequential phases:

• **Security**: Define tiered strategy, prioritize risks, and execute value-driven projects aligned to OKRs and business outcomes.

• **Visibility**: Build a reliable picture of assets, data flows, and control performance while exposing shadow IT and blind spots.

• **Administration**: Embed governance, ownership, change management, and metrics for sustained success and continuous improvement.

2. Pillar I — Security

We begin with comprehensive discovery: networks, endpoints, identities, data flows, and business objectives. By reviewing the current threat landscape and organizational mission, we collaborate to develop a tiered security strategy and maintain a backlog of value-driven projects aligned to corporate OKRs and risk-based priorities.

Key Practices

• Threat modeling and comprehensive risk assessment (NIST CSF Identify; ISO/IEC 27005)

• Architecture baselining (SSE/SASE/Zero Trust), identity & access hardening, MFA implementation

• Data protection strategy (CASB/DLP), email security hardening, phishing resistance programs

• Secure SDLC: requirements definition, threat modeling, code review, SAST/DAST, SBOM, supply-chain controls

Outcomes

• Prioritized roadmap with clear owners, timelines, and budgets

• Defined policies and standards supporting risk acceptance and exception processes

• Improved control maturity measured against CIS Controls and NIST CSF

3. Pillar II — Visibility

We expand and validate the comprehensive inventory of assets, identities, data stores, vendors, and applications. We assess monitoring depth and coverage, measure the true attack surface, and systematically uncover shadow IT. We translate technical findings into executive language: risk appetite, Key Risk Indicators (KRIs), and quantified business impact.

Key Practices

• Attack Surface Management (ASM): external discovery, SaaS sprawl identification, exposed services catalog

• Asset & identity inventory management, CMDB hygiene, comprehensive vendor risk catalog

• Control effectiveness validation: SIEM/XDR detection capabilities, logging depth, telemetry quality assessment

• Shadow IT and risky application triage (CASB/DLP); policy enforcement and exception workflow management

Outcomes

• Executive dashboards expressing risk in business terms with defined KRIs and thresholds

• Comprehensive evidence for compliance and audits; gap tracking and remediation SLAs

• Significant reduction of unknown assets and blind spots; improved detection coverage metrics

4. Pillar III — Administration

Administration represents persistence—the organizational capability to maintain improvements over time. We establish robust governance structures, clear roles and responsibilities, effective change management processes, and continuous improvement mechanisms to ensure results persist well beyond the initial project window.

Key Practices

• Governance framework: steering committee structure, comprehensive policies/standards, exception management processes

• Operating model design: RACI matrices, service catalog development, intake processes, prioritization, and change control

• Metrics & reporting systems: OKRs definition, KRIs monitoring, audit readiness, comprehensive post-incident reviews

• Training & enablement programs: role-based education, secure engineering playbooks, awareness campaigns

Outcomes

• Sustained compliance posture and comprehensive auditability

• Reduced MTTR through well-rehearsed playbooks and clear ownership structures

• Continuous improvement feedback loops integrated with leadership cadence

5. Mapping to Standards & Frameworks

Our methodology aligns comprehensively with widely adopted frameworks to ensure portability, auditability, and industry best practice compliance:

Framework & Standard	Usage and Application in Our Methodology
NIST Cybersecurity Framework 2.0	Identify, Protect, Detect, Respond, Recover — serves as our comprehensive top-level operating model and stra
NIST SP 800-53 & 800-171	Comprehensive control baselines specifically designed for federal data and contractors; directly maps to enterp
ISO/IEC 27001 & 27002	Information Security Management System (ISMS) governance framework and detailed control catalog that supp
CIS Critical Security Controls v8	Prioritized safeguards specifically designed to close the most common security gaps quickly and effectively with
SOC 2 (AICPA TSC)	Trust Services Criteria for service organizations covering security, availability, confidentiality, processing integrit
PCI DSS	Industry-specific controls for organizations handling cardholder data and payment processing with strict complia
MITRE ATT&CK	Comprehensive adversary technique knowledge base used to guide threat detection and security testing progra
OWASP Top 10 / ASVS / SAMM	Application security risks catalog, verification standards, and software assurance maturity model for comprehen
ENISA Guidelines	European Union-aligned best practices for comprehensive risk management and organizational resilience with f

6. Metrics, OKRs, and Executive Reporting

We systematically convert security activities into measurable business outcomes. Our approach includes leading and lagging indicators that provide actionable insights for executive decision-making:

• **OKR Example**: Reduce phishing risk exposure by 40% in two quarters (measured by: click-rate ↓, report-rate ↑, time-to-report ↓).

• **Key Risk Indicators**: % of unmanaged SaaS applications; % of high-risk third parties without current assessment; % of endpoints without EDR coverage.

• **MTTR/MTTD Metrics**: Mean Time to Detect and Mean Time to Respond using SIEM/XDR platforms and standardized playbooks.

• **Control Coverage**: Logging depth and quality, identity MFA adoption rates, DLP policy coverage, patch management SLA compliance.

Executive dashboards translate these technical metrics into business trends, performance targets, and data-driven budget justification.

7. Operating Model & RACI

A well-defined operating model accelerates decision-making and ensures accountability. The following RACI matrix illustrates high-level responsibilities for key cybersecurity capabilities:

Capability	Responsible	Accountable	Consulted	Informed
Security Strategy	CISO	CIO/CTO	Business Unit Leads	Board of Directors
Risk Register	Risk Manager	CISO	Legal, Finance	All Staff
Identity & Access	IAM Lead	CISO	HR, App Owners	Internal Audit
Data Protection	Data Security Lead	CISO	Privacy, BU Owners	Legal Counsel
Incident Response	IR Team Lead	CISO	IT Operations, PR	Board of Directors

R = Responsible, A = Accountable, C = Consulted, I = Informed

8. 90-Day Example Roadmap

The following timeline represents a typical 90-day engagement structure, with each phase building upon previous accomplishments while maintaining focus on immediate value delivery:

Days 0–30: Foundation & Discovery

• Project kickoff, stakeholder alignment, and comprehensive threat/risk baseline establishment

• Complete asset & identity inventory; establish Attack Surface Management (ASM) baseline

• Implement quick wins: enforce MFA across all systems, email security hardening initiatives

Days 31–60: Strategy & Implementation

• Develop prioritized roadmap with defined budgets; establish governance framework and steering committee

• Launch DLP/CASB policies pilot program; implement logging depth improvements across critical systems

• Conduct incident response playbook development and execute first tabletop exercise

Days 61–90: Optimization & Handover

• Deploy executive dashboard version 1; finalize OKRs and KRI thresholds with leadership team

• Complete shadow IT application triage and implement policy exception workflow

• Deliver roadmap version 2 and comprehensive handover plan for sustained operations

9. References & Further Reading

Our methodology draws from industry-leading frameworks and standards. The following resources provide additional context and detailed implementation guidance:

• NIST Cybersecurity Framework 2.0 - Framework for Improving Critical Infrastructure Cybersecurity

• NIST Special Publication 800-53 Revision 5 - Security and Privacy Controls for Information Systems

• NIST Special Publication 800-171 - Protecting Controlled Unclassified Information in Nonfederal Systems

• ISO/IEC 27001:2022 - Information Security Management Systems Requirements

• ISO/IEC 27002:2022 - Information Security, Cybersecurity and Privacy Protection

• CIS Critical Security Controls Version 8 - A Defense-in-Depth Set of Best Practices

• SOC 2 Trust Services Criteria - AICPA Service Organization Control Reports

• MITRE ATT&CK; Framework - Adversarial Tactics, Techniques & Common Knowledge

• OWASP Top 10, Application Security Verification Standard (ASVS), and Software Assurance Maturity Model (SAMM)

• ENISA Threat Landscape Reports - European Union Agency for Cybersecurity

• PCI Data Security Standard (DSS) Version 4.0 - Payment Card Industry Security Requirements