

PROPOSAL FOR COMPREHENSIVE CYBERSECURITY ASSESSMENT AND SERVICES

*San Bernardino County Employees' Retirement Association
(SBCERA) July 24, 2025*

Prepared By:
Symosis Security LLC
Ivan Trusevych, Account Manager
(310) 999-8263
consulting@symosis.com

Symosis Security | 1250 Borregas Ave, Sunnyvale, CA 94089

Table of Contents

| | |
|--|-----------|
| Cover Letter | 3 |
| Summary Response (Appendix C – Questionnaire Responses) | 5 |
| Executive Summary | 16 |
| Introduction..... | 17 |
| SBCERA Context and Readiness Summary..... | 18 |
| Company Background..... | 19 |
| Past Performance Highlights..... | 22 |
| Scope OF Service..... | 23 |
| 1. Cybersecurity Compliance Assessment | 24 |
| 2. Penetration Testing & Technical Security Assessment..... | 24 |
| 3. AI Governance & Security Audit | 25 |
| 4. Purple Team Exercises | 25 |
| 5. Retesting of Remediated Findings | 25 |
| 6. IT Governance & Risk Management Review | 25 |
| 7. Data Protection & Privacy Review..... | 26 |
| Optional Services (Future Phases or Add-Ons)..... | 26 |
| Approach..... | 27 |
| Our Risk Assessment Philosophy | 27 |
| Framework-Guided Risk Assessment Approach..... | 29 |
| Industry Standards and Frameworks Utilized | 29 |
| Planning & Kickoff..... | 29 |
| Communication & Stakeholder Alignment | 30 |
| Methodology | 30 |
| Cybersecurity Compliance Assessment..... | 30 |
| Penetration Testing & Technical Security Assessment..... | 32 |
| AI Governance & Security Audit | 33 |
| Purple Team Exercise | 34 |
| Retest of Remediated Findings..... | 35 |
| IT Governance & Risk Management Review..... | 35 |
| Data Protection & Privacy Review | 36 |
| Optional Services Execution Overview..... | 37 |
| Deliverables Summary..... | 39 |
| Assumptions..... | 39 |
| Project Delivery Plan | 40 |

| | |
|---|-----------|
| Staffing And Qualification..... | 41 |
| Core Team Roles & Credentials | 41 |
| Team Attributes | 42 |
| Bios & Staffing Flexibility | 42 |
| Fixed Fee AND Core Service Scope | 42 |
| Included Core Service Areas | 42 |
| Fixed Fee Also Includes | 43 |
| Optional Services (Future Phases or Add-Ons)..... | 43 |
| Blended Hourly Rate Schedule | 43 |
| Conclusion | 43 |
| Appendix A: Staff Bios | 44 |
| Appendix B: Request for Qualifications Signature Page..... | 36 |

Cover Letter

To: SBCERA Evaluation Committee

From: Symosis Security LLC

Date: July 21, 2025

Subject: Proposal Submission – SBCERA Comprehensive Cybersecurity Assessment and Services

Dear Evaluation Committee,

Symosis Security is pleased to submit this updated proposal in response to SBCERA's Request for Qualifications for Comprehensive Cybersecurity Assessment and Services. We have carefully reviewed SBCERA's responses to vendor inquiries and have updated our materials to reflect the clarified scope, requirements, and expectations.

We understand the importance of safeguarding member data, ensuring regulatory alignment, and building operational resilience. Our updated response directly addresses:

- The expectation for **in-person board presentations** of audit results
- Coverage for up to **500 devices**, **3–5 web applications**, and a **hybrid cloud environment** with ~30 SaaS tools and ~35 accounts
- Evaluation of SBCERA's **AI governance policy** and use of generative AI tools
- Development of a **data classification policy** and support for **NIST/HIPAA/ISO framework selection**
- Social engineering simulations focused on **phishing campaigns** and tailored security awareness
- Optional delivery of **training sessions, tabletop exercises, and policy development**

Our updated proposal includes the following components:

- Comprehensive Proposal outlining updated scope, methodology, and deliverables
- Appendix A: Confirmation of Compliance with Minimum Qualifications
- Appendix B: Signed Signature Page
- Appendix C: Revised Questionnaire Responses (aligned to clarified requirements)

Symosis accepts all the Terms and Conditions and contract requirements outlined in the SBCERA Comprehensive Cybersecurity Assessment and Services solicitation as well as its addendums "as-is" and will be able to meet/exceed all the government's solicitation requirements. We appreciate the opportunity to support SBCERA's

cybersecurity goals and stand ready to begin work within two weeks of selection. Please don't hesitate to contact us with any follow-up questions or clarification needs.

Sincerely,

A handwritten signature in black ink, appearing to be 'Kartik Trivedi', with a stylized, cursive script.

Kartik Trivedi
Partner, Symosis Security LLC
consulting@symosis.com | (213) 248-1130

Summary Response (Appendix C – Questionnaire Responses)

Symosis has provided a summary response to each of the seven (7) questions outlined in **Appendix C**. At the end of each response, we've included references to the relevant section(s) containing more detailed explanations. Feel free to use the Acrobat bookmark feature to navigate into each section.

1. A brief written description of the Firm's approach to the project.

Symosis employs a **proven, standards-aligned methodology** grounded in years of hands-on experience across public-sector, enterprise, and cloud-native environments. Our approach emphasizes **thorough planning, transparent execution, and risk-aligned recommendations** that are tailored to SBCERA's mission, fiduciary responsibilities, and operational realities.

Our Risk Assessment Philosophy

We believe cybersecurity risk assessments must go beyond checklists and compliance snapshots. Our model is built on four foundational pillars:

1. **Mission-Aligned Evaluation**
Assessment criteria are directly aligned to SBCERA's fiduciary and operational goals—ensuring outcomes are practical, contextual, and risk-based.
2. **Framework-Agnostic, Outcome-Driven**
While NIST CSF forms our baseline, we incorporate controls and benchmarks from ISO 27001, HIPAA, GDPR, and NIST SP 800-53/171, based on regulatory applicability and control depth needs. This enables us to build a roadmap that's both actionable and compliant.
3. **Quantitative and Qualitative Insight**
We provide control maturity scorecards, risk heatmaps, and executive-ready summaries, balancing data-driven scoring with strategic insights for board and technical audiences.
4. **Continuous Improvement Orientation**
Our assessments are structured to establish a repeatable model for long-term remediation tracking, re-testing, and framework benchmarking.

Assessment Activities and Process

| Stage | Activities |
|-----------------------|---|
| Discovery & Interview | Conduct interviews with IT, legal, compliance, and leadership stakeholders to understand priorities, roles, and risk ownership. |
| Artifact Collection | Review policies, org charts, diagrams, audit logs, SaaS inventories, and risk registers. |
| Control Mapping | Align existing controls to relevant frameworks (NIST CSF, ISO 27001, HIPAA, GDPR, 800-53/171). |

| | |
|-------------------------|--|
| Gap & Maturity Analysis | Evaluate control design and operational effectiveness using Symosis' 5-point scoring model. |
| Risk Register | Build a ranked risk register factoring likelihood, impact, and mitigation readiness across strategic, IT, and compliance layers. |
| Roadmap Creation | Develop a prioritized remediation plan with owner mapping, estimated effort, and milestones. |

Framework Flexibility

Based on SBCERA's regulatory footprint and systems in use, we may map controls to:

- **NIST CSF** – Foundational for public-sector
- **NIST SP 800-53/171** – For deeper technical and control rigor
- **ISO 27001** – For governance and certification alignment
- **HIPAA** – For any health or member data implications
- **GDPR** – For personal data privacy if applicable

The final deliverables will include multi-framework mappings where applicable.

Sample Outputs & Deliverables

- Control Gap Matrix mapped to NIST, ISO, HIPAA, and GDPR
- Maturity scorecards by function
- Risk severity heatmaps
- Remediation roadmap with timelines and owners
- Executive-ready summary report

Standards and Tools We Leverage

- **Frameworks:** NIST CSF, ISO 27001/27701, HIPAA, GDPR, PCI-DSS, CCPA
- **Security Testing Standards:** OWASP Top 10, ASVS, MITRE ATT&CK, PTES, OSSTMM
- **Tools:** Nessus, Burp Suite, Microsoft Secure Score, LogicManager, Wireshark, Metasploit

This structured, flexible, and outcome-driven methodology will ensure SBCERA receives not just an assessment but a governance-aligned, forward-looking cybersecurity maturity model.

See: *Cybersecurity Compliance Assessment, Project Delivery Plan, and Risk Assessment Philosophy* in the Proposal.

2. Please describe the firm's typical approach to similar projects.

Symosis follows a consistent, modular, and repeatable methodology for delivering cybersecurity assessments to public-sector organizations, retirement systems, and regulated entities. Our approach is structured into clearly defined phases with an emphasis on stakeholder alignment, risk-contextualized control evaluation, and practical remediation planning.

Typical Phases of Execution

1. Planning & Kickoff

- Conduct kickoff meeting with key stakeholders (IT, compliance, legal, executive leadership).
- Establish communication cadence, points of contact, and documentation handoff schedules.
- Confirm scope, testing boundaries, risk tolerances, and reporting preferences.

2. Discovery & Evidence Collection

- Gather security policies, network diagrams, org charts, risk registers, SaaS/app inventories.
- Document key workflows, control ownership, and exception handling procedures.

3. Control Mapping & Maturity Scoring

- Align collected evidence and observed controls with NIST CSF, ISO 27001, HIPAA, and other applicable frameworks.
- Score each domain using Symosis' 5-level maturity rubric to assess design and operational effectiveness.

4. Technical Testing (if in scope)

- Perform internal/external vulnerability scans, phishing simulations, wireless testing, and cloud config reviews.
- Tools used may include Nessus, Burp Suite, Nmap, PowerShell, Microsoft Secure Score, and others.

5. Risk Register Development

- Identify and rank risks based on likelihood, impact, and current mitigation readiness.
- Include both technical and non-technical risks (e.g., vendor access, policy gaps, MFA exceptions).

6. Remediation Roadmap & Executive Briefing

- Develop an actionable roadmap organized by quick wins, mid-term improvements, and strategic initiatives.
- Provide visualizations, heatmaps, and summaries designed for both technical and board-level audiences.
- Conduct final walkthrough meeting and presentation with stakeholders.

What Sets Our Approach Apart

- **Outcome-Driven:** Beyond control mapping, we prioritize outcomes tied to real risk reduction.
- **Communication-Centric:** Weekly touchpoints, live trackers (if desired), and responsive escalation channels.
- **Framework-Flexible:** We tailor control analysis to NIST CSF, ISO 27001, HIPAA, GDPR, or hybrid approaches based on each client's needs.
- **Technology-Informed:** Integrating posture insights from tools like Microsoft Purview, Azure, and SaaS admin panels to provide modern coverage.

This methodology has been successfully applied in engagements for county retirement systems, public pension funds, and state agencies—ensuring a balance of rigor, clarity, and actionability.

See: *Methodology by Service Area, Execution Plan, and Workstream Descriptions* in the Proposal.

3. Please provide a written description of the Firm's approach to the challenge and scope of work provided in Part 1.

Symosis understands that SBCERA requires a comprehensive, multi-dimensional cybersecurity assessment that not only satisfies compliance requirements, but also supports long-term resilience, fiduciary responsibility, and executive-level transparency.

We approach this challenge through a blended strategy that incorporates compliance alignment, technical testing, AI risk governance, and policy support—all tailored to SBCERA's hybrid cloud infrastructure, evolving threat landscape, and regulatory profile.

Scope Areas and Our Approach

1. Cybersecurity Risk & Compliance Assessment

- Leverage NIST CSF and ISO 27001 as the foundation while incorporating HIPAA, NIST 800-53/171, and GDPR where relevant.
- Conduct interviews with IT, compliance, and executive teams to understand control ownership and operational risk.
- Map existing controls to selected frameworks and assess maturity using our 5-point rubric.
- Provide a detailed roadmap with milestones, estimated effort, and responsible owners.

2. Technical Penetration Testing

- Test up to 500 assets (devices, servers, cloud services) as specified in the Q&A clarification.
- Include external, internal, wireless, and phishing testing to simulate real-world threats.

- Use OWASP, PTES, and MITRE ATT&CK-aligned tactics to identify exploitable weaknesses.
- Deliver attack chain diagrams, PoCs, and clear remediation guidance.

3. Application and SaaS Review

- Assess 3–5 web applications and ~30 SaaS tools in use.
- Conduct configuration reviews, session management analysis, and admin privilege checks.
- Provide a SaaS risk heatmap based on vendor risk, access hygiene, and misconfiguration severity.

4. AI Governance & GenAI Tool Review

- Evaluate SBCERA's AI governance policy maturity and adoption of tools like Microsoft Copilot or ChatGPT.
- Assess risks around data leakage, adversarial inputs, prompt injection, and hallucination.
- Deliver a Responsible AI Governance Framework with threat modeling and usage control recommendations.

5. Data Classification Policy Support

- Collaborate with SBCERA to draft or enhance its data classification policy.
- Identify gaps in current schema, tagging practices, and associated access/restriction controls.
- Recommend data lifecycle policies (retention, deletion, encryption) based on best practices.

6. Remediation Roadmap & Presentation

- Build a board-ready report with a prioritized roadmap, policy recommendations, and control maturity baselines.
- Deliver an **in-person presentation to the SBCERA board** to communicate findings and answer questions.

Key Clarifications Incorporated from the RFP Q&A

- Coverage includes **500 endpoints**, **3–5 web applications**, and **~30 SaaS tools**
- **In-person board presentation** is expected and confirmed as part of our deliverables
- Evaluation of SBCERA's **AI governance policy** and use of **generative AI tools** is explicitly addressed

- Optional services including **training, tabletop exercises, and policy development** are available upon request

Symosis has delivered similar full-scope assessments for pension systems, unions, and public entities and is equipped to guide SBCERA through a meaningful, risk-based cybersecurity maturity engagement.

See: *Scope Clarification Updates, Engagement Overview, and Workstream Details* in the Proposal.

4. The team's expertise assembled by the Firm to carry out the work.

Symosis has assembled a senior-led team with deep experience in cybersecurity assessments, compliance frameworks (NIST, ISO, HIPAA), offensive security, cloud environments, and AI risk governance. Each team member brings relevant domain expertise and public-sector experience, ensuring SBCERA receives informed, context-aware, and high-quality support across all components of the engagement.

Key Personnel Assigned to the Project

Kartik Trivedi – Partner & Lead Advisor

- **Certifications:** CISSP, CISA, CISM
- **Experience:** 20+ years leading cybersecurity programs for federal agencies, pension funds, and SaaS enterprises
- **Focus Areas:** Executive advisory, compliance mapping, GRC, AI security, stakeholder engagement
- **Relevance:** Will serve as SBCERA's primary contact, lead roadmap development, and conduct board presentation

Clinton Mugge – Partner, Governance & Threat Oversight

- **Certifications:** CISSP
- **Experience:** Former counterintelligence officer; 20+ years in cyber governance and enterprise risk
- **Focus Areas:** Threat modeling, risk register development, third-party risk, executive workshops
- **Relevance:** Will lead risk identification and drive mission-aligned recommendations

Tinatini Sandroshvili – Senior Engineer, Technical Testing Lead

- **Certifications:** CEH, CySA+
- **Experience:** Extensive background in red/purple team operations, ISO/SOC2 audit support, and vulnerability assessments

- **Focus Areas:** Internal/external network testing, phishing simulations, wireless assessment, control gap validation
- **Relevance:** Will lead penetration testing and develop exploit documentation and technical deliverables

Dave Patel – Senior Manager, Compliance & Data Risk

- **Certifications:** (Pursuing ISO Lead Implementer; extensive internal audit experience)
- **Experience:** GRC practitioner with deep experience in vendor risk management, privacy compliance (HIPAA, GDPR), and control audits
- **Focus Areas:** Data classification policy, AI governance gap analysis, SaaS posture review
- **Relevance:** Will support documentation analysis and policy development

Team Capabilities and Tools

- Familiarity with public retirement system environments and compliance obligations
- Experience delivering in-person board-level presentations and executive briefings
- Proficiency in tools such as Nessus, Burp Suite, Metasploit, Microsoft Purview, PowerShell, Wireshark, and LogicManager
- Understanding of stakeholder dynamics between IT, Compliance, and Executive teams

All work will be led and performed by U.S.-based staff. If specialized AI or cloud architecture support is needed, we may draw from a vetted internal bench (with prior public-sector experience), subject to SBCERA approval.

See: Appendix A – Staff Bios and Staffing and Qualifications in the Proposal.

5. Please summarize five similar projects in progress or completed in the last 3 years.

Symosis has supported numerous public-sector clients, retirement systems, and regulated organizations in conducting cybersecurity assessments, penetration tests, and governance reviews. Below are five highly relevant engagements:

1. KCERA – Kern County Employees' Retirement Association

- **Client:** Public pension fund under California's 1937 Act
- **Scope:** Full cybersecurity risk assessment, HIPAA/NIST framework mapping, and roadmap development
- **Activities:** Stakeholder interviews, policy review, endpoint testing, SaaS risk evaluation, board presentation
- **Outcome:** Delivered board-ready report, framework-aligned roadmap, and risk register; currently serving as ongoing trusted advisor

- **Relevance to SBCERA:** Similar governance model and compliance needs

2. IBEW-NECA Trust Funds

- **Client:** Multi-union health and pension fund
- **Scope:** Multi-year managed security and compliance support
- **Activities:** HIPAA compliance audit, phishing simulations, security awareness training, risk scoring
- **Outcome:** Reduced social engineering risk, improved audit readiness, integrated remediation planning
- **Relevance to SBCERA:** Strong focus on compliance, privacy, and fiduciary oversight

3. LinkedIn (Microsoft)

- **Client:** Global enterprise with sensitive data, cloud-native infrastructure, and GenAI adoption
- **Scope:** Security posture assessments, SSPM integrations, and AI governance framework development
- **Activities:** Custom tooling for API posture, risk modeling, SaaS controls validation, policy evaluation
- **Outcome:** Delivered a live GenAI governance model, continuous risk dashboarding, and security automation
- **Relevance to SBCERA:** Provides maturity perspective and AI governance insights applicable to SBCERA's GenAI usage

4. State Bar of California

- **Client:** Regulatory agency handling legal licensing and complaints
- **Scope:** Cyber risk and compliance audit, vendor risk program review
- **Activities:** ISO 27001-based audit, access control review, data retention and encryption assessments
- **Outcome:** Produced control gap matrix, policy enhancement roadmap, and executive summary
- **Relevance to SBCERA:** Demonstrates public-sector risk prioritization and control maturity evaluation

5. NASA (via Federal Subcontractor)

- **Client:** Federal aerospace agency (under a larger integrator)
- **Scope:** Internal controls audit and cloud governance evaluation
- **Activities:** Framework mapping to NIST 800-53, SaaS tool assessments, IT risk interviews, maturity scoring

- **Outcome:** Validated internal controls and delivered cross-mapped roadmap under stringent federal protocols
- **Relevance to SBCERA:** Demonstrates ability to work within strict compliance and technical testing boundaries

6. Teachers' Retirement System (TRS) of the City of New York

- **Client:** One of the largest public pension funds in the U.S., with over \$100 billion in assets under management
- **Scope:** Multi-workstream cybersecurity support engagement (2025–2026), including compliance assessments, custom integrations, SSPM posture reviews, and 24x7 managed services
- **Activities:**
 - NIST CSF and ISO-aligned security assessments
 - Custom API posture integrations into Adaptive Shield
 - Application and SaaS security reviews (400+ apps)
 - Executive reporting and monthly board deliverables
- **Outcome:** Delivered structured remediation plans, maturity scoring, and real-time risk insights; supporting continuous improvement of TRS's security program
- **Relevance to SBCERA:** Closely aligned organizational structure and oversight expectations; demonstrates Symosis' ability to manage large, complex, and high-impact public-sector engagements

7. Intuit Inc.

- **Client:** Fortune 500 financial technology company serving millions of global users
- **Scope:** Long-standing engagement (10+ years) supporting red teaming, penetration testing, and application security for cloud-native and financial platforms
- **Activities:**
 - Application penetration tests across critical financial services and platforms
 - Internal red teaming and adversary simulation engagements
 - API, mobile, and cloud (AWS, GCP) security testing
 - Collaboration with Intuit's internal security and product engineering teams
- **Outcome:** Helped continuously validate and harden applications and infrastructure; contributed to Intuit's strong security reputation in the financial services sector
- **Relevance to SBCERA:** Demonstrates Symosis' ability to deliver rigorous testing, adapt to evolving architectures, and operate as a trusted long-term partner

Each of these engagements required coordination across technical and executive stakeholders, careful alignment to compliance frameworks, and the development of actionable risk roadmaps—skills and experience that will directly benefit SBCERA.

See: *Past Performance Highlights* in the Proposal.

6. Identify all staff and any subcontractors who will be assigned to work on the project.

Symosis will assign a **core team of senior staff**, with **one of the key personnel serving as lead** based on project timing and availability. This lead will be supported by other qualified team members to ensure all deliverables are met on schedule and to the highest quality standards.

All team members listed below are Symosis employees or partners. **No subcontractors will be used.**

Key Personnel Pool

| Name | Role | Primary Expertise |
|------------------------------|------------------------------------|--|
| Kartik Trivedi | Partner & Engagement Lead | Executive advisory, risk assessment, board presentations |
| Clinton Mugge | Partner, Risk & Governance Lead | Cyber risk, threat modeling, policy maturity |
| Tinatini Sandroshvili | Senior Engineer & Testing Lead | Penetration testing, network security, purple team exercises |
| Dave Patel | Senior Consultant, Compliance & AI | AI governance, data classification, SaaS and policy review |

One of the above individuals will lead the engagement depending on final scheduling, supported by additional team members for specific workstreams such as penetration testing, SaaS configuration reviews, or policy development.

- All staff are **U.S.-based**, experienced in public-sector cybersecurity, and cleared for sensitive work.
- We may deploy additional internal SMEs (e.g., AI tooling, secure SDLC) as needed—subject to SBCERA’s approval.
- **No subcontractors or third-party vendors** will participate in project delivery.

See full staff bios and qualifications in Appendix A – Key Personnel of the Proposal.

7. Please identify if your firm or any proposed subcontractors have any real or potential conflicts of interest in performing the requested services.

Symosis Security **does not have any real or potential conflicts of interest** in performing the requested services for SBCERA.

- We are an **independent cybersecurity advisory and testing firm** and do not resell or promote any third-party software, tools, or platforms.
- We have **no financial interests, fiduciary relationships, or business arrangements** with any of SBCERA's vendors, service providers, or affiliated agencies.
- We do not subcontract any work to third parties without prior client consent and none are proposed for this engagement.
- All personnel assigned to the project are direct employees or partners of Symosis, and we maintain **strict internal confidentiality protocols** for public-sector clients.

If any potential conflict were to arise during the course of the engagement (e.g., if we are engaged by another public pension fund with overlapping vendors or systems), we will **promptly disclose** it to SBCERA in writing and take all necessary steps to avoid influence or bias.

Executive Summary

Engagement Objective

SBCERA seeks a cybersecurity partner to conduct a full-spectrum cybersecurity assessment spanning internal systems, cloud infrastructure, policies, and emerging risk domains. This engagement is intended to strengthen regulatory alignment, uncover exploitable vulnerabilities, and equip SBCERA to advance its security, privacy, and operational resilience posture.

Symosis at a Glance

- 15+ years serving public-sector organizations, pension systems, and regulated industries
- Proven track record with clients like **KCERA**, **NASA**, **State Bar of California**, and **LinkedIn**
- Deep expertise in NIST, ISO 27001, HIPAA, GDPR, and SaaS/cloud security frameworks
- Specialists in AI governance, risk automation, and penetration testing
- Senior-led delivery model with U.S.-based and global engineering teams

Scope of Work

Our fixed-fee engagement includes:

- Compliance Gap Analysis mapped to NIST CSF, NIST 800-53/171, HIPAA, ISO 27001, and GDPR
- Internal and External Penetration Testing across up to 500 assets
- Web Application Testing of 3–5 applications, including authenticated/grey-box assessments
- Wireless Security Assessment for <10 SSIDs at SBCERA's single San Bernardino location
- Cloud Configuration Review, covering Microsoft 365, Azure AD, and ~30 SaaS tools across ~35 accounts
- AI Governance Review focused on SBCERA's recently adopted policy and current GenAI use
- Purple Team Simulation Exercise to test real-time detection and response (no blue team currently in place)
- Retesting of Remediated Findings with validation reporting
- IT Governance and Privacy Assessment, including data classification support

Deliverables

- Executive Summary and board-ready reporting
- Detailed technical assessment reports
- Cross-mapped control gap analysis and compliance roadmap
- AI policy review and risk gap summary
- Draft data classification schema (if needed)
- In-person presentation to the SBCERA Board at engagement conclusion
- Weekly updates and critical issue escalations

Timeline

- Project Duration: ~14–18 weeks
- Engagement Start: Within 2 weeks of award
- Final Deliverables: Delivered on-site to the Board with optional follow-up sessions

Pricing

- Fixed Fee: \$96,000 for core services
- Optional Services: Billed separately at \$165/hour (e.g., phishing simulation, policy development, tabletop exercises)
- Includes up to 3 on-site visits; travel beyond that billed at cost

Introduction

SBCERA is undertaking a strategic initiative to assess and enhance its cybersecurity, governance, and risk management practices. As a public pension system operating under the 1937 Act, SBCERA must balance stringent fiduciary responsibility with modern digital service delivery—spanning on-premises infrastructure, hybrid cloud deployments, SaaS tools, and emerging technologies such as generative AI.

Symosis Security is well-positioned to support this effort. We bring over 15 years of cybersecurity consulting experience with public-sector and quasi-governmental organizations across California and beyond. Notably, we have served pension systems like KCERA and municipal agencies such as the State Bar of California, delivering actionable insights across compliance, threat detection, and operational risk domains.

Through this engagement, Symosis will provide SBCERA with a comprehensive cybersecurity assessment covering:

- Internal and external technical posture (up to 500 assets)
- Web applications (3–5), including authenticated testing
- Microsoft 365, Azure AD, and a hybrid SaaS environment (~30 tools, ~35 accounts)
- Wireless and perimeter exposure
- Governance maturity, policy coverage, and data classification readiness
- Review of the recently adopted AI governance policy and GenAI use cases
- Simulation-based Purple Team exercises (with support for Blue Team maturity)
- Retesting of remediated vulnerabilities for closure validation

SBCERA has communicated through the Q&A process that it values vendor flexibility, in-person board presentations, and assistance in selecting the most relevant security frameworks. Our approach responds to that by combining hands-on technical testing, risk-informed governance review, and framework-aligned advisory services to deliver both strategic and operational value.

Symosis understands the nuances of pension systems' infrastructure, staffing, and compliance needs. We focus not just on identifying risk—but on providing the structure, tools, and support needed to remediate effectively and prepare for future audits, reviews, or board inquiries.

We are confident in our ability to deliver a successful engagement and support SBCERA as a long-term security partner.

SBCERA Context and Readiness Summary

Symosis has reviewed SBCERA's RFP and the detailed responses provided through the vendor Q&A process. The following table summarizes the current cybersecurity posture, infrastructure profile, and expectations outlined by SBCERA. This understanding has directly informed our scope, methodology, and delivery approach.

| Category | Key Insights |
|-----------------------------------|--|
| Organizational Profile | Fewer than 100 employees; single location in San Bernardino, CA |
| Infrastructure Scope | Up to 500 devices including routers, switches, firewalls, servers, access points, desktops, and laptops |
| Testing Expectations | Internal and external penetration testing prioritized; 3–5 web applications (up to 200 dynamic pages); focus on pension administration system and edge/perimeter systems |
| Compliance Requirements | Attempting to follow NIST CSF, NIST 800-53/171, HIPAA, GDPR, ISO 27001; expects vendor support in confirming most relevant frameworks |
| Cloud & SaaS Environment | Hybrid model with <30 SaaS applications , ~35 cloud accounts, 1 Windows domain; mixed cloud platform usage (Azure, M365, others); source code review excluded |
| AI Usage & Policy | Limited GenAI usage (e.g., Copilot); AI governance policy recently adopted ; no AI/ML models to be tested |
| Communication Requirements | Weekly progress updates; immediate notification of high-risk or critical findings |
| Board Reporting | Final results must be presented in person to the SBCERA Board or its appointed committee |
| Data Classification | No formal classification policy in place; vendor expected to assist in development |
| Blue Team Support | No formal blue team in place; vendor expected to provide simulation support, detection feedback, and response framework |
| Security Awareness & IR Exercises | Phishing simulation expected (1–2 per year); annual tabletop exercises to begin post-initial audit |
| Framework Alignment | Flexible and collaborative; vendor to lead control mapping and framework selection discussions |

Company Background

Symosis Security is a specialized cybersecurity consultancy with over **20 years of experience** helping organizations strengthen risk management, ensure regulatory compliance, and securely adopt emerging technologies. Founded in 2004, Symosis combines deep cybersecurity expertise with cutting-edge AI/ML capabilities—enabling clients to defend against today’s threats while modernizing how security, compliance, and governance are operationalized.

Our team includes engineers, AI specialists, and cybersecurity leaders who have built and led programs at Fortune 100 companies, public pension systems, and global technology firms. Today, we apply that expertise to help organizations design secure architectures, automate governance workflows, and assess risks across hybrid environments—including Microsoft 365, Azure, cloud-native SaaS, and AI-integrated platforms.

Symosis is a **California-certified Small Business** headquartered in the **San Francisco Bay Area**, with delivery teams across the **U.S., India, and Europe**. We operate with a **lean, senior-led model** to ensure responsiveness, technical depth, and accountability throughout every engagement.

Core Focus Areas

- **AI and Automation for Risk and Threat Management**
- **Compliance Readiness** (NIST CSF, NIST 800-53/171, ISO 27001, HIPAA, CIS, PCI)
- **SaaS Security Posture Management (SSPM)**
- **Penetration Testing & Application Security**
- **Microsoft 365, Azure, and AWS Security Hardening**
- **Virtual CISO Services & Policy Development**
- **Managed Cybersecurity Operations (SOC/SIEM/SOAR)**

Why Clients Choose Symosis

- **Expert-Led Delivery:** Our team includes CISSP, CISM, GCIA, CEH, and ISO 27001 Lead Auditors—as well as authors of industry-defining resources like *Hacking Exposed*.
- **Public Sector & Pension System Experience:** We’ve supported NASA, the State Bar of California, Los Angeles County, and multiple public retirement systems with audits, risk assessments, and regulatory compliance.
- **Proven in SaaS & AI Security:** Our consultants have led global cloud and AI risk programs at platforms like LinkedIn and Autodesk, helping define controls for LLMs, GenAI, API security, and automation governance.
- **Tool-Agnostic Approach:** We operate within the client’s preferred tech stack—leveraging tools like InsightIDR, CrowdStrike, and ServiceNow—without introducing proprietary systems or ingesting sensitive data.

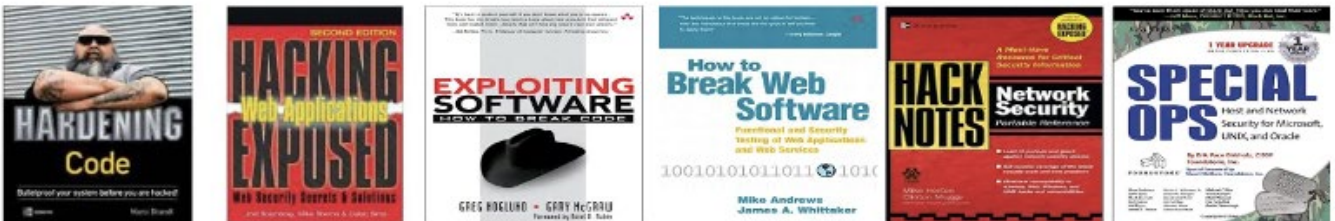
- ## Credentials and Certifications

- C|CISO, CISSP, CISM, CEH, GCIA, CCSP, HCISPP

- CISA, CBCP

- Microsoft Certified: Azure Security Engineer Associate
- Certified AI/ML Engineers

- **Authors & Contributors:** Contributors to *Hacking Exposed*, *Cloud Security Handbook*, and multiple SANS training modules
- **Industry Speakers:** Presenters at RSA, Black Hat, OWASP, ISSA, and ISACA global events
- **Professional Leadership:** Board members at ISACA Silicon Valley; advisors to cybersecurity education and workforce development programs



- **Public Sector:** NASA, Los Angeles County, State Bar of California, California Office of Emergency Services

- **Retirement Systems:** Kansas City Employees' Retirement System (KCERS), Teachers' Retirement System of NYC (TRS), [other engagements anonymized for confidentiality]
- **Tech Sector:** LinkedIn, Autodesk, Smartsheet
- **Healthcare & Finance:** Accession Risk, HealthStream, multiple regional healthcare networks



Past Performance Highlights

Symosis has supported a diverse set of public-sector, retirement, and regulated industry clients with cybersecurity assessments, AI governance, penetration testing, and compliance advisory services. The following engagements are directly aligned with SBCERA's scope—including experience with the 1937 Act, NIST-based assessments, M365 and Azure hardening, and in-person board reporting.

KCERA – Kern County Employees' Retirement Association

- **Scope:** Multi-year cybersecurity risk assessment, penetration testing, and governance support
- **Services:** Policy development, technical testing, compliance mapping (NIST, HIPAA), executive reporting
- **Value:** Trusted advisor to one of California's largest 1937 Act pension funds; ongoing advisory partner

IBEW-NECA Trust Funds

- **Scope:** SOC implementation and Microsoft 365 security enhancement
- **Services:** MDR/SIEM integration, phishing simulations, M365 hardening, user training
- **Value:** Established full-spectrum monitoring with a financial warranty-backed support model

TRS – Teachers' Retirement System of the City of New York

- **Scope:** Cybersecurity strategy development and 24x7 monitoring program launch
- **Services:** MSSP onboarding, Rapid7 and CrowdStrike integration, AI-enabled SOC workflows, board dashboard design
- **Value:** Designed and implemented end-to-end public-sector cybersecurity roadmap with automation and executive metrics

State Bar of California

- **Scope:** Risk advisory and enterprise vulnerability management
- **Services:** Penetration testing (OWASP Top 10), static/dynamic code reviews, control gap analysis
- **Value:** Delivered FY2024 cybersecurity roadmap and board-aligned remediation guidance

NASA – Johnson Space Center

- **Scope:** Mission-critical risk assessment under NIST 800-53A
- **Services:** Control validation, risk assessment, ISS system mapping, OMB A-130 reporting

- **Value:** Evaluated 1,000+ assets under a \$100K federal engagement; aligned findings with NIST and NASA internal frameworks

LinkedIn (Microsoft)

- **Scope:** GenAI risk governance and third-party security automation
- **Services:** Custom AI agent development, vendor risk workflow automation, SSPM integration
- **Value:** Embedded GenAI into security operations at enterprise scale; ongoing partnership in SaaS risk automation

Intuit

- **Scope:** Global threat modeling and continuous vulnerability management
- **Services:** Risk triage, remediation planning, third-party analysis, intelligence integration
- **Value:** Supported threat and risk operations for a global financial SaaS environment

Accession Risk Management Group

- **Scope:** Enterprise risk governance, AI policy implementation, M365 compliance
- **Services:** PHI risk validation in Teams, DLP review, ServiceNow automation roadmap
- **Value:** Delivered AI policy framework and compliance strategy for a health-regulated organization

Logitech

- **Scope:** SaaS security posture review and AI tool threat modeling
- **Services:** SSPM audit, AI use-case mapping, LLM-related threat modeling
- **Value:** Operationalized internal AI security guardrails and improved SaaS visibility

Harley-Davidson Financial Services

- **Scope:** DevSecOps assessment and application security
- **Services:** OWASP ASVS-based app testing, vendor security review, SDLC controls
- **Value:** Uncovered critical risks in third-party platforms and enabled SDLC maturity planning

Scope OF Service

Symosis will deliver a comprehensive cybersecurity assessment and advisory engagement tailored to SBCERA's needs, emphasizing measurable risk reduction,

regulatory alignment, and long-term operational resilience. The following services are based directly on the RFP and vendor Q&A responses, and can be executed in parallel or sequentially over a 10–14 week phased engagement:

Scope Parameters Summary (based on RFP + Q&A responses)

Symosis' scope and pricing are based on the following confirmed parameters, as clarified through SBCERA's published Q&A:

| Category | Detail |
|------------------------|--|
| Users / Employees | < 100 users (single-site organization) |
| Devices in Scope | Up to 500 endpoints, servers, network devices |
| Web Applications | 3–5 externally facing web applications (200 pages max; may include pension admin system) |
| Wireless Networks | Fewer than 10 SSIDs at the San Bernardino facility |
| Cloud / SaaS Platforms | Microsoft 365, Azure AD, and ~30 SaaS applications across ~35 cloud accounts |
| Domain Scope | Single Windows domain |
| Blue Team Maturity | No formal blue team in place (requires advisory support during purple team exercise) |
| AI Usage | Light GenAI use (e.g., Microsoft Copilot); AI policy adopted in 2024 |
| Board Presentation | Final results to be presented in person to SBCERA's Board or designated committee |
| Data Classification | No formal schema in place; vendor support requested to develop one |

This scope profile directly informs our proposed testing methodology, team assignments, and fixed fee.

1. Cybersecurity Compliance Assessment

Evaluate SBCERA's alignment with frameworks including **NIST CSF, NIST 800-53/171, HIPAA, GDPR, and ISO 27001**. This includes documentation review, stakeholder interviews, control maturity scoring, gap analysis, and delivery of a **framework crosswalk and compliance roadmap**. Symosis will assist in identifying the most appropriate frameworks based on SBCERA's mission, data types, and operational structure.

2. Penetration Testing & Technical Security Assessment

Perform internal and external penetration testing across up to **500 IP-based assets** (endpoints, servers, network devices, cloud services) and **3–5 web applications**, including authenticated testing with multiple user roles. Assessment scope includes:

- Internal network security testing

- External perimeter review
- Web app testing aligned with OWASP and business logic abuse
- Wireless security testing for <10 SSIDs at a single San Bernardino site
- Cloud configuration testing for Microsoft 365, Azure AD, and major SaaS platforms
- Activities aligned with OWASP, PTES, and MITRE ATT&CK

3. AI Governance & Security Audit

Review SBCERA's **recently adopted AI governance policy** and evaluate current GenAI usage (e.g., productivity tools like Copilot). Assessment focuses on:

- AI policy coverage, transparency, and accountability
- Risk of prompt injection, data leakage, or model misuse
- Privacy and compliance concerns related to AI use
- No model testing or adversarial training required
- Deliverables include a **policy gap review and governance recommendations**

4. Purple Team Exercises

Conduct collaborative attack simulations to assess SBCERA's detection and response readiness. Given the absence of a formal blue team, Symosis will:

- Define realistic scenarios based on current threat intelligence
- Execute non-disruptive, rules-of-engagement-bound red team activity
- Evaluate log detection, escalation, and triage performance
- Provide coaching and improvement recommendations to IT staff
- Support future blue team capacity-building efforts

5. Retesting of Remediated Findings

Conduct follow-up testing on previously identified vulnerabilities or gaps. Symosis will:

- Validate whether remediation actions have been properly implemented
- Provide verification evidence and residual risk commentary
- Deliver a "remediation status" report with closure tracking

6. IT Governance & Risk Management Review

Assess SBCERA's current IT governance structure, policies, and alignment with risk management practices. This includes:

- Evaluation of board reporting, decision rights, and oversight
- Policy gap analysis (incident response, DR/BCP, vendor risk)
- Role/responsibility matrix
- Strategic roadmap for governance improvement

7. Data Protection & Privacy Review

Evaluate SBCERA's current data protection and privacy practices including:

- Access controls, MFA coverage, and privileged access
- Encryption of data in transit and at rest (AES, TLS)
- Data retention, secure deletion practices, and privacy controls
- Development of a **draft data classification policy** and sensitivity schema
- Alignment with HIPAA and GDPR expectations

Optional Services (Future Phases or Add-Ons)

Symosis offers a robust portfolio of optional services that can be activated either during this engagement or in future phases. These offerings are designed to help SBCERA scale its cybersecurity maturity, automation, and resilience through targeted assessments, tooling, and advisory support. All services are scoped collaboratively based on need, timing, and budget.

Optional Services by Category

Risk & Compliance Services

- **Security Awareness & Phishing Simulations** – Deliver 1–2 simulated phishing campaigns annually, paired with staff training focused on real-world social engineering tactics.
- **Incident Response Tabletop Exercises** – Facilitate scenario-driven tabletop sessions to test leadership roles, decision-making, and communications during crises (e.g., ransomware, data breach).
- **Policy & Procedure Development** – Draft or refine cybersecurity policies aligned to NIST and ISO standards (IR, access control, third-party oversight, acceptable use).
- **Third-Party Risk Management & Continuous Monitoring** – Conduct vendor security reviews, control mapping, and implement automation for ongoing due diligence.
- **Security Maturity & GRC Advisory** – Provide board-level program roadmaps, risk register updates, and governance structure evaluations across NIST CSF, ISO 27001, and HIPAA.

Security Engineering & Implementation

- **Microsoft 365 / Azure Hardening** – Review and enhance configurations across Exchange, SharePoint, Teams, Defender, and Azure identity controls based on CIS Benchmarks and Secure Score.

- **Secure Tool & Architecture Deployments** – Implement Zero Trust models, secure SDLC enhancements, and security automation across on-prem/cloud environments.
- **Secure SDLC Review** – Evaluate custom/internal software development workflows for DevSecOps maturity, secure coding, and change control discipline.

AI & Automation Enablement

- **AI Governance Integration & Workflow Automation** – Automate risk and policy workflows using ServiceNow, Power Automate, or Azure Logic Apps, aligned to SBCERA's AI policy.
- **AI Risk Scanning & Tool Deployment** – Deploy tools and dashboards to monitor AI-enhanced processes, data handling, and GenAI usage across business workflows.

Offensive Security Services

- **Red Team & Custom Threat Simulations** – Design and execute tailored adversary emulation exercises based on SBCERA's threat model and asset landscape.
- **Custom Tabletop Scenario Development** – Develop replayable tabletop scenarios for use in annual simulations and internal drills.

Incident Response & Reporting

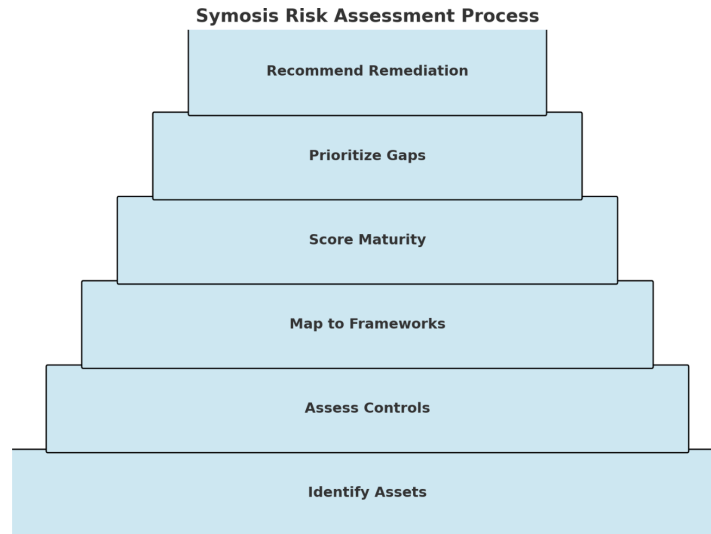
- **Incident Response Plan & Runbook Creation** – Build scenario-specific IR playbooks (e.g., ransomware, phishing, insider threats) and escalation maps for technical and executive audiences.
- **Cybersecurity Metrics & Dashboard Design** – Define KPIs and KRIs for internal tracking and board reporting; design mock dashboards using Excel or Power BI.

Approach

Symosis employs a proven, standards-aligned methodology grounded in years of hands-on experience across public-sector, enterprise, and cloud-native environments. Our methodology emphasizes thorough planning, transparent execution, and risk-aligned recommendations tailored to SBCERA's mission, regulatory context, and operational realities.

Our Risk Assessment Philosophy

At Symosis, we believe cybersecurity risk assessments should go beyond checklists and static reports. Our approach is built on four pillars:



1. **Mission-Aligned Evaluation**

We align our assessment criteria to SBCERA's fiduciary and operational responsibilities—ensuring recommendations are practical and risk-based.

2. **Framework-Agnostic, Outcome-Driven**

While we leverage NIST CSF as a foundational structure, we incorporate elements of ISO 27001, HIPAA, and GDPR where needed. This allows us to deliver an actionable roadmap regardless of the specific regulatory lens.

3. **Quantitative and Qualitative Insight**

We combine maturity scoring, heatmaps, and control ratings with strategic insights and board-level narratives to empower both technical and non-technical leadership.

4. **Continuous Improvement Orientation**

Rather than a one-time snapshot, our process sets up SBCERA with a model for long-term tracking, remediation validation, and framework benchmarking.

Sample outputs include:

- Control maturity scorecards
- Risk severity heatmaps
- Framework-specific mappings
- Prioritized remediation plan with owner/timeline tracking

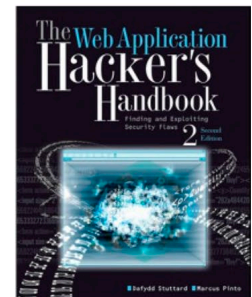
Framework-Guided Risk Assessment Approach

Symosis will work closely with SBCERA to determine the most appropriate cybersecurity frameworks to guide the assessment. While our baseline approach leverages NIST CSF and ISO 27001, we adapt to client needs by incorporating elements from NIST 800-53/171, HIPAA, GDPR, or proprietary controls. This flexible methodology ensures that the resulting risk register, control analysis, and roadmap reflect both best practices and SBCERA's operational context. The final deliverables will present maturity-level scoring, risk rankings, and actionable recommendations mapped to multiple frameworks when applicable.

Industry Standards and Frameworks Utilized

We base our assessments on the most recognized cybersecurity methodologies and frameworks, including:

- **OWASP Top 10, OWASP ASVS** – Secure coding and web application testing
- **PTES** – Penetration Testing Execution Standard
- **MITRE ATT&CK** – Adversary tactics and techniques simulation
- **NIST SP 800-42, 800-115, 800-171, CSF** – Compliance and risk management
- **OSSTMM** – Open-Source Security Testing Methodology Manual
- **ISO/IEC 27001, 27701** – Governance and control maturity
- **CIS Benchmarks, Microsoft Secure Score** – Cloud infrastructure hardening
- **HIPAA, PCI DSS, GDPR, CCPA** – Regulatory frameworks



Planning & Kickoff

Prior to testing and evaluation, Symosis will conduct a formal kickoff session with SBCERA stakeholders to align objectives, validate scope, and establish communication protocols. Activities include:

- Reviewing current documentation, architecture diagrams, and user roles
- Validating credentials, access keys, and system coverage
- Establishing **Rules of Engagement (ROE)** for all testing
- Identifying points of contact and escalation paths
- Finalizing the schedule, logistics, and expected deliverables

Communication & Stakeholder Alignment

Symosis ensures project success through structured and transparent communications:

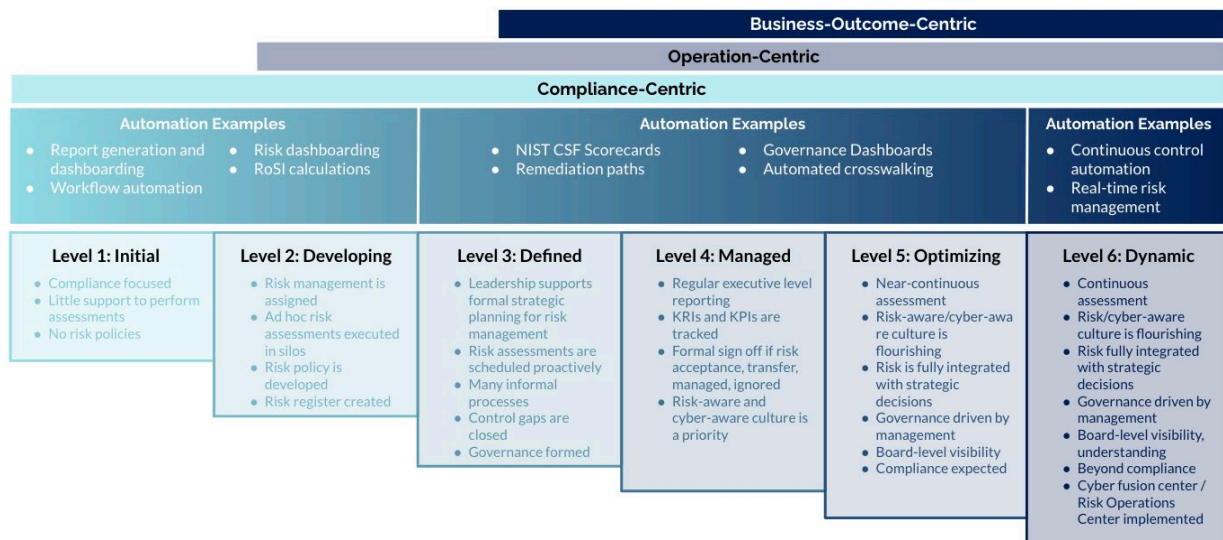
- Weekly check-in calls and written progress summaries
- Single point of contact (SPOC) assigned by Symosis
- Shared task tracker (if preferred) for live status updates
- Issue escalation and resolution pathways with SLA alignment

Symosis employs a proven, standards-aligned methodology grounded in years of hands-on experience across public-sector, enterprise, and cloud-native environments. Our methodology emphasizes thorough planning, transparent execution, and risk-aligned recommendations tailored to SBCERA's mission, regulatory context, and operational realities.

Methodology

Cybersecurity Compliance Assessment

This workstream serves as the foundation for understanding SBCERA's current security posture and regulatory alignment. Symosis uses a **risk-informed, outcome-driven compliance methodology**—not just mapping controls to frameworks, but evaluating control effectiveness, residual risk, and governance maturity across people, process, and technology.



Activities & Process

| Stage | Activities |
|-----------------------|--|
| Discovery & Interview | Meet with IT, compliance, legal, and executive stakeholders to understand current priorities, risks, and control responsibilities. |

| | |
|---------------------------|--|
| Artifact Collection | Gather policies, procedures, network diagrams, risk registers, audit logs, org charts, and SaaS/cloud inventories. |
| Control Mapping | Map current controls to relevant frameworks (NIST CSF, ISO 27001, HIPAA, GDPR, 800-53/171) based on SBCERA's risk profile. |
| Gap & Maturity Analysis | Use Symosis' 5-point scoring model to evaluate control design and operational effectiveness across domains. |
| Risk Register Development | Build a risk register ranking threats by likelihood, impact, and mitigation readiness—covering IT, compliance, and strategic layers. |
| Roadmap Creation | Develop a remediation roadmap with control owners, milestones, estimated effort, and supporting recommendations. |

Framework Flexibility

Based on SBCERA's regulatory footprint and systems, Symosis may recommend mapping to:

- **NIST CSF** (foundational framework for U.S. public-sector alignment)
- **NIST 800-53 / 800-171** (for technical control depth)
- **ISO 27001** (for governance maturity and certification alignment)
- **HIPAA** (for data protection, especially in member health records)
- **GDPR** (where applicable for personal data privacy governance)

Final deliverables will reflect whichever frameworks are most applicable to SBCERA, based on discussion during kickoff.

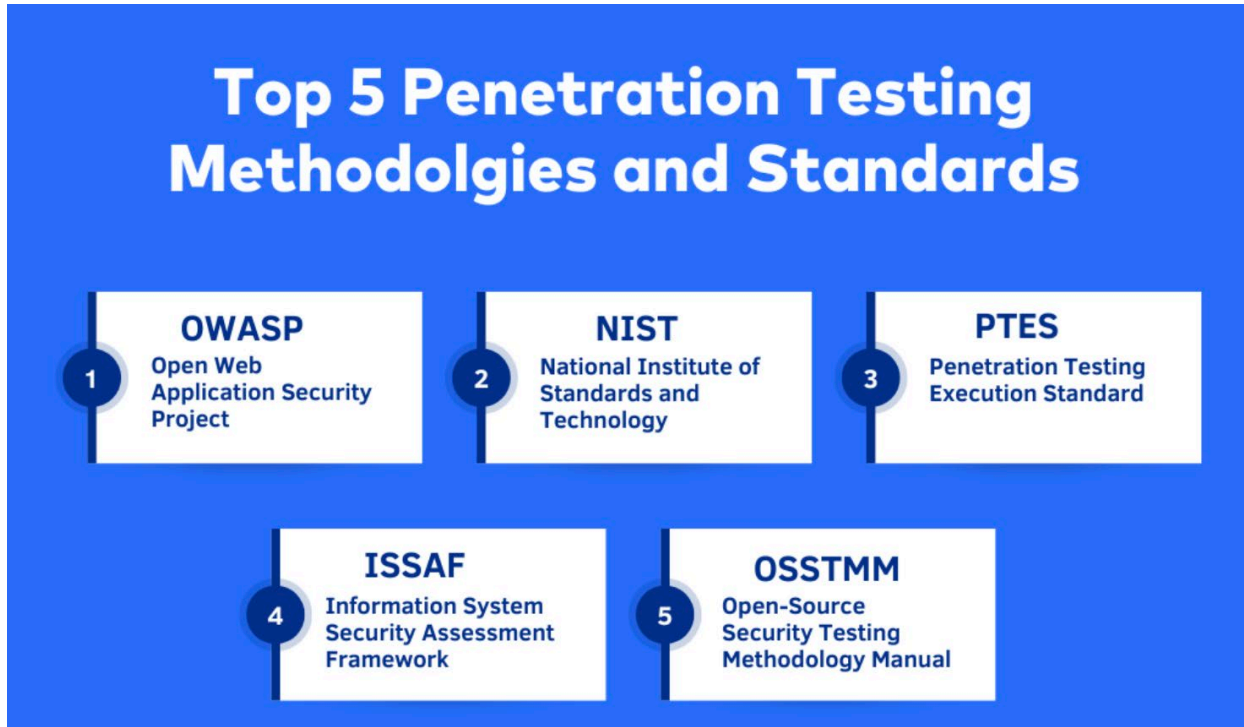
| Assessment Output | NIST CSF | NIST 800-53/171 | ISO 27001 | HIPAA | GDPR |
|---------------------------------------|----------|-----------------|-----------|-------|------|
| Control Gap Analysis | ✓ | ✓ | ✓ | ✓ | ✓ |
| Maturity Scorecard | ✓ | ✓ | ✓ | | |
| Risk Register | ✓ | ✓ | ✓ | ✓ | ✓ |
| Compliance Roadmap | ✓ | ✓ | ✓ | ✓ | ✓ |
| Policy Recommendations | ✓ | ✓ | ✓ | ✓ | ✓ |
| Final Executive Summary Report | ✓ | ✓ | ✓ | ✓ | ✓ |

Deliverables

- Cross-mapped **Control Gap Matrix** (NIST, ISO, HIPAA, GDPR)
- **Control Maturity Scorecard** by function
- Prioritized **Compliance Roadmap** with accountability matrix
- **Risk Register** with technical and procedural threat alignment
- Executive-ready **Summary Report** for board consumption

Penetration Testing & Technical Security Assessment

Symosis approaches testing not as a checkbox exercise but as a threat-informed assessment to identify real-world exploitable vulnerabilities and help SBCERA understand both technical exposures and business impact.



Activities & Process

| Stage | Activities |
|-------------------------------------|---|
| Scoping & Target Definition | Define in-scope IPs, apps, endpoints, wireless assets, and external surfaces. |
| Reconnaissance & Mapping | Identify exposed services, DNS records, weak certificates, and misconfigurations. |
| Exploitation & Privilege Escalation | Execute exploits and lateral movement tests in a controlled, rule-bound environment. |
| Web Application Testing | Conduct business logic abuse, OWASP Top 10 checks, and session handling reviews. |
| Wireless Network Testing | Test for rogue access points, WPA/WPA2 misconfigurations, and MAC spoofing risks. |
| Cloud Posture Review | Assess Azure AD, Microsoft 365, and SaaS configs for open access, excessive privileges, or Shadow IT. |

Tools & Techniques

- **Tools:** Burp Suite, Nmap, Metasploit, BloodHound, PowerShell, Wireshark
- **Approach:** Aligned with MITRE ATT&CK and PTES standards

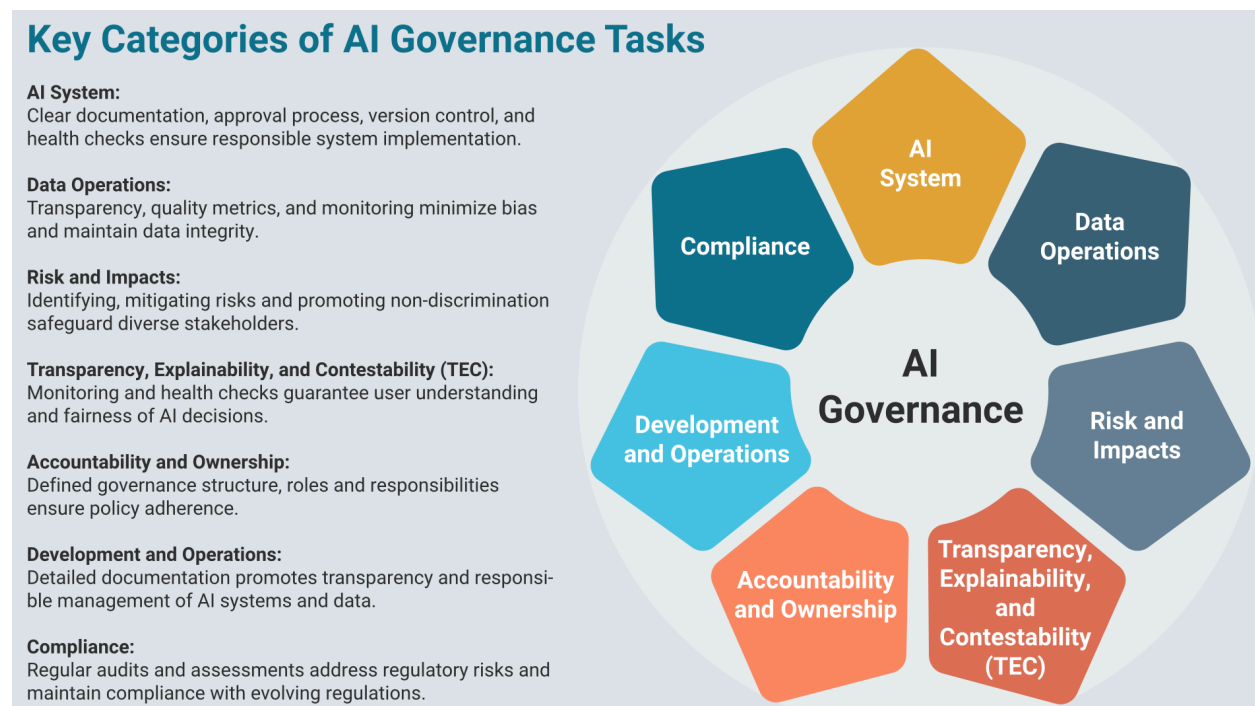
- **Constraints:** API and mobile testing **not in scope** unless redefined in future phases

Deliverables

- Detailed **Technical Vulnerability Report** with impact ratings
- **Proof-of-Concepts** (PoCs), screenshots, and exploit trails
- **Attack Chain Diagrams** and lateral movement visualizations
- **Remediation Recommendations** by category and estimated effort

AI Governance & Security Audit

As SBCERA has adopted an AI governance policy and uses GenAI tools for productivity, Symosis will assess the alignment, risk exposure, and policy maturity related to AI tool usage.



Activities & Process

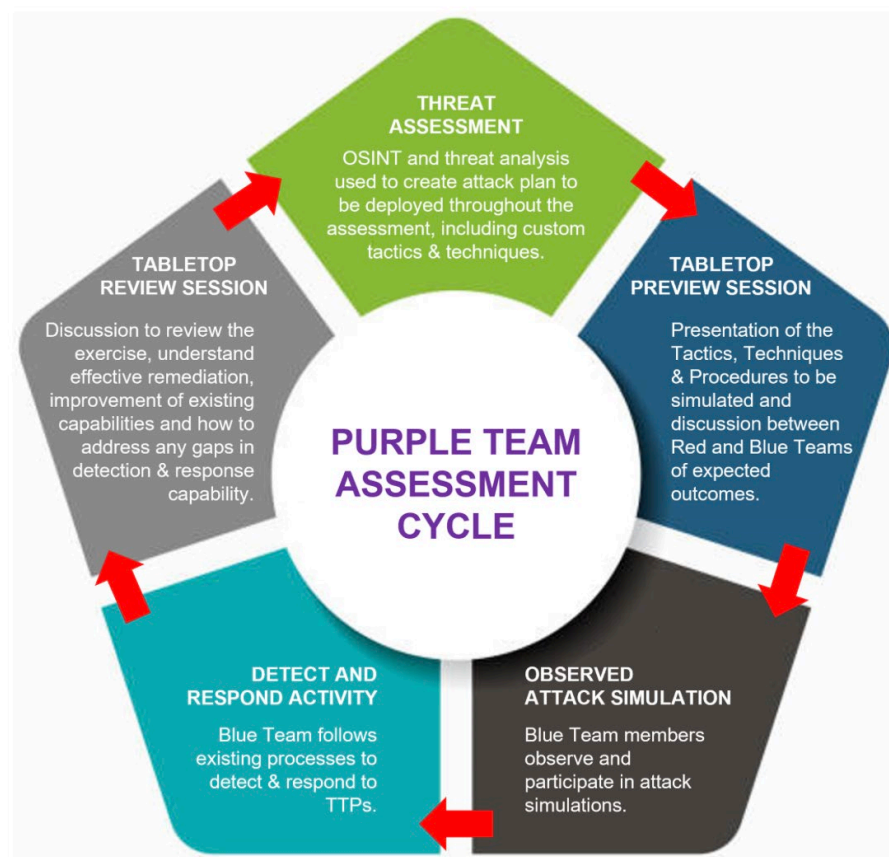
| Stage | Activities |
|----------------------------|--|
| AI Inventory | Document GenAI tools, model integrations, and in-use platforms (e.g., Copilot, ChatGPT). |
| Governance Review | Assess policy coverage around AI use, ownership, auditability, and transparency. |
| Security Controls Review | Evaluate risks from adversarial inputs, model exfiltration, prompt injection, and hallucination. |
| Privacy & Data Risk Review | Analyze exposure of PII, PHI, or sensitive content to external or unvetted models. |

Deliverables

- AI risk and governance gap assessment
- Responsible AI Governance Framework (draft policy)
- AI-specific threat model visual
- Recommendations for monitoring and data use controls

Purple Team Exercise

This collaborative engagement simulates a real attack to test and improve detection, response, and communication workflows within SBCERA's environment. Our red team executes a safe, defined set of attack scenarios while the blue team observes and responds.



Activities & Process

| Stage | Activities |
|---------------------------|--|
| Scenario Design | Define attack type (e.g., credential theft, phishing, lateral movement) and ROE. |
| Red Team Execution | Simulate attacker behavior using live or replayed payloads and tactics. |

| Stage | Activities |
|------------------------------|--|
| Blue Team Observation | SBCERA's IT/security team monitors logs, detects activity, and responds in real time. |
| Post-Exercise Debrief | Review timeline, missed detections, and response times to develop improvement actions. |

Deliverables

- Simulation scenario narrative and execution timeline
- Detection and response effectiveness dashboard
- Recommendations for detection logic and IR playbook refinement

Retest of Remediated Findings

Symosis conducts a targeted validation of previously reported vulnerabilities or issues that SBCERA has remediated, to ensure closure and reduce lingering risk.

Activities & Process

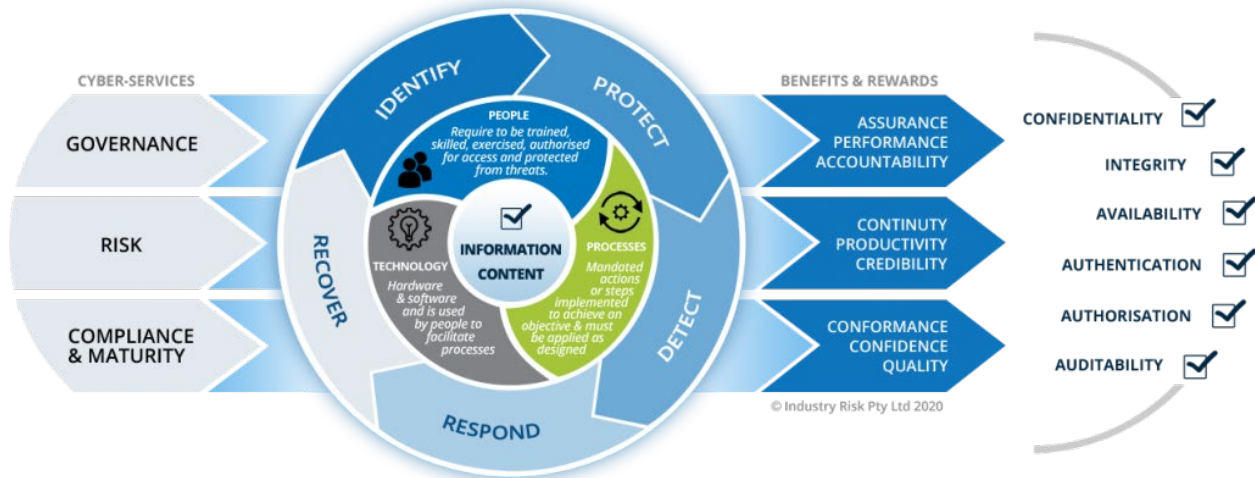
| Stage | Activities |
|--------------------------------------|--|
| Verification Scope Definition | Identify issues marked as resolved or partially mitigated. |
| Targeted Retesting | Re-run previous exploit or misconfiguration test cases using updated parameters. |
| Change Documentation | Collect evidence of remediation, configuration changes, or control improvements. |

Deliverables

- Updated vulnerability report with remediation status (Closed / Partial / Open)
- Change logs and verification screenshots
- Residual risk commentary and re-mitigation guidance (if needed)

IT Governance & Risk Management Review

This service evaluates SBCERA's governance maturity—how cyber risks are tracked, escalated, and owned across leadership levels—and whether policies are aligned to the enterprise's mission and fiduciary responsibilities.



| Stage | Activities |
|------------------------------------|---|
| Governance Structure Review | Assess board reporting, risk ownership, CISO alignment, and decision rights. |
| Policy Coverage Analysis | Evaluate coverage of incident response, change management, DR/BCP, and vendor risk. |
| Strategic Alignment Review | Compare current cyber risk priorities to organizational goals and operations. |

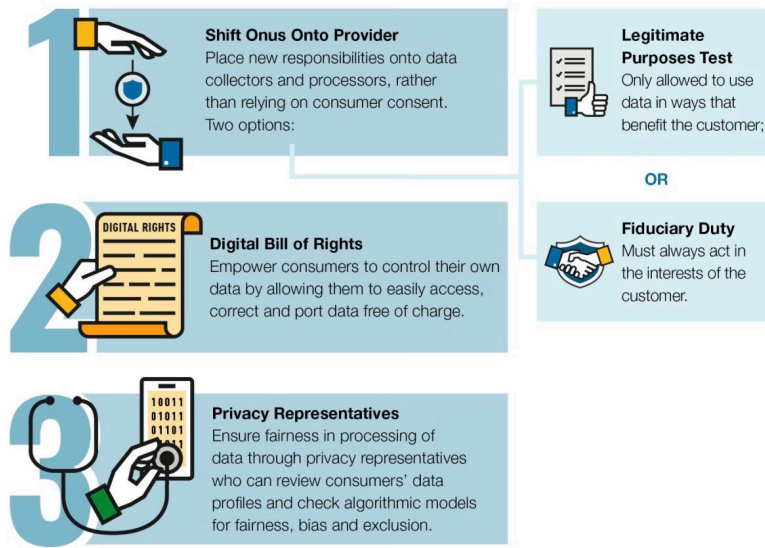
Deliverables

- Governance effectiveness review report
- Role/responsibility matrix
- Policy enhancement roadmap
- Strategic alignment map (if misalignment is observed)

Data Protection & Privacy Review

This service evaluates SBCERA's ability to protect sensitive data—across classification, access control, encryption, retention, and privacy compliance.

Three Ways to Modernize Data Privacy and Protection



Activities & Process

| Stage | Activities |
|---|---|
| Data Classification Review | Review data schema or help define one (if missing). |
| Access Control Evaluation | Check MFA enforcement, privileged access logging, and RBAC usage. |
| Encryption & Retention Audit | Evaluate encryption at rest/in-transit, retention policies, and deletion hygiene. |
| Privacy Risk Evaluation | Align practices with HIPAA and GDPR obligations based on data types handled. |

Deliverables

- Data protection maturity model
- Encryption and access control effectiveness report
- Privacy compliance recommendations and policy gaps

Optional Services Execution Overview

Symosis offers the following optional services as standalone engagements or logical extensions of the primary assessment.

| Optional Service | Purpose | Key Outputs / Deliverables |
|--|--|---|
| Security Awareness Training & Phishing Simulations | Deliver targeted simulations (1–2/year) and end-user training to reduce social engineering risk. | Training materials, phishing metrics, risk trend report |
| Incident Response Tabletop Exercises | Simulate ransomware, breach, or outage scenarios to evaluate | Scenario guide, facilitation deck, after- |

| | | |
|---|--|---|
| | SBCERA's IR coordination and response. | action report, IR plan updates |
| Secure SDLC Review | Assess software development lifecycle maturity, focusing on security design and DevSecOps practices (if applicable). | SDLC maturity checklist, process gaps, secure coding guidance |
| Policy & Procedure Development | Draft or refine cybersecurity policies aligned to NIST CSF and ISO 27001. | Policy templates (IR, access, vendor, acceptable use), approval roadmap |
| Third-Party Risk Management & Continuous Monitoring | Assess vendor security controls and automate ongoing third-party risk reviews. | Vendor risk register, control mapping, automation workflows |
| Security Maturity & GRC Advisory | Define long-term security roadmap and governance practices to mature SBCERA's program. | Maturity model, control roadmap, board-ready GRC summary |
| Secure Tool & Architecture Deployment | Design and implement secure architecture and automation workflows, including Zero Trust and cloud hardening. | Reference architectures, deployment plan, security controls matrix |
| Microsoft 365 & Azure Hardening | Harden M365 and Azure services like Exchange, Teams, Defender, SharePoint, and identity. | Hardening checklist, Secure Score deltas, config baselines |
| AI Governance Integration & Workflow Automation | Automate risk workflows and enforce AI policy compliance using Power Automate, ServiceNow, or Logic Apps. | Configured workflows, governance logic, user training |
| AI Risk Scanning & Tool Deployment | Deploy AI-informed tools to monitor workflows and identify risk signals across business operations. | Risk alerts, dashboard integration, AI policy alignment summary |
| Red Team & Custom Threat Simulations | Execute advanced threat emulation and design scenarios for tabletop or live Purple Team exercises. | Red Team scripts, attack paths, detection feedback report |
| Incident Response Plan & Runbook Creation | Create role-specific playbooks for threats like ransomware, phishing, and insider abuse. | IR playbooks, escalation workflows, contact matrix |
| Cybersecurity Metrics & Dashboard Design | Build KPIs/KRIs and dashboards for IT leadership and Board reporting. | Metrics catalog, mock dashboard, reporting schedule |

Deliverables Summary

For each core service area, Symosis will deliver both standard engagement-wide outputs and service-specific artifacts. These are designed to inform technical teams, support remediation efforts, and enable board-level decision-making.

Standard Deliverables (applies to all service areas):

- **Technical Report** detailing findings, methodologies, evidence, and tailored recommendations
- **Weekly Updates** summarizing progress, open items, and identified risks
- **Preliminary Findings** shared early to enable timely remediation
- **Executive Summary** suitable for board and senior leadership presentation

Service-Specific Deliverables

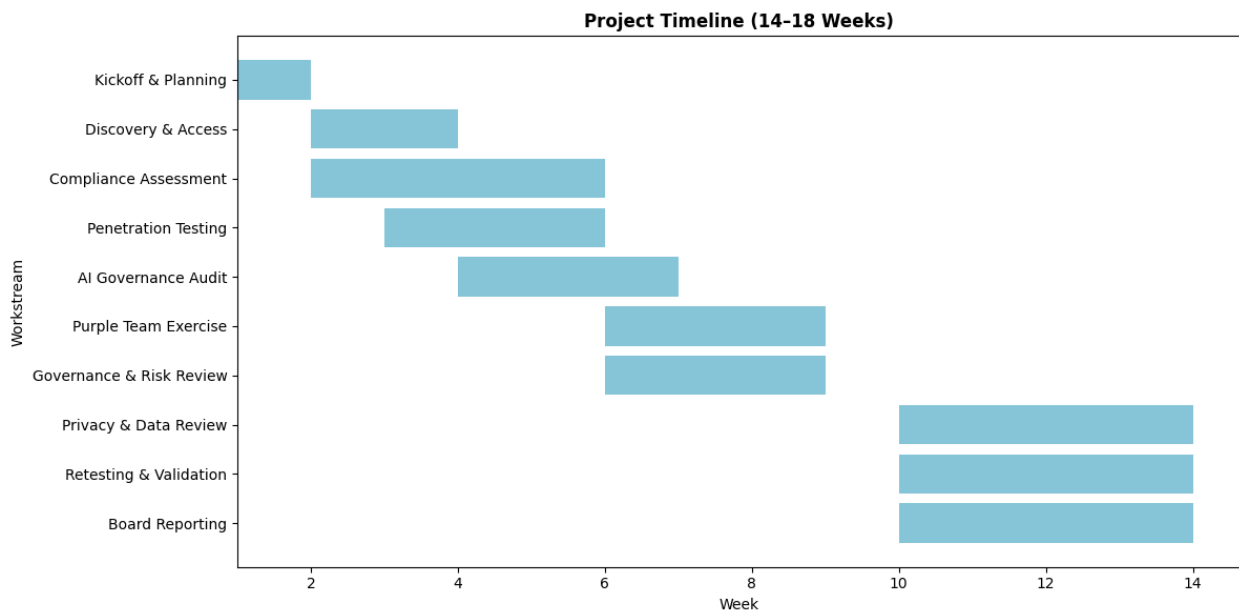
| Service Area | Key Deliverables |
|---|---|
| Compliance Assessment | - Gap analysis matrix against NIST CSF, HIPAA, ISO 27001, etc. - Control maturity scorecard - Prioritized compliance roadmap |
| Penetration Testing | - Vulnerability report with severity scoring and supporting evidence - Exploitation proof-of-concepts (PoCs) - Attack chain diagrams and remediation guidance |
| AI Security Audit | - AI governance policy and risk gap analysis - AI/ML threat model and evaluation checklist - Inventory of AI use cases and associated risks |
| Purple Team Exercise | - Scenario execution narrative and timeline - Detection & response effectiveness dashboard - Updated IR playbooks and improvement plan |
| Retesting of Findings | - Remediation status report (Closed / Partially Resolved / Open) - Validation evidence - Residual risk summary |
| IT Governance Review | - Role and responsibility matrix - Governance documentation review - Strategic recommendations and alignment roadmap |
| Privacy & Data Protection Review | - Data classification and lifecycle mapping - Encryption and access control assessment - HIPAA/GDPR compliance recommendations tailored to SBCERA |

Assumptions

1. SBCERA will assign appropriate points of contact for coordination, approvals, and technical access.
2. Remote access will be permitted for discovery, interviews, and testing where feasible; physical access will be provided as needed for on-site testing or presentations.

3. Confidential and sensitive data will be handled in accordance with SBCERA's data security and retention policies. All such data will be securely stored, transmitted, and deleted post-engagement as required.
4. Necessary technical documentation (e.g., IP ranges, network diagrams, application lists) will be provided following contract execution and governed by a mutual non-disclosure agreement (NDA).
5. SBCERA and Symosis will mutually agree on the applicable cybersecurity frameworks to guide the compliance assessment during project kickoff.
6. All project-related communications, deliverables, and milestone approvals will follow a weekly check-in cadence, with escalation paths documented in the kickoff phase.

Project Delivery Plan



| Phase | Weeks | Updated Activities |
|--------------------------|-----------|---|
| Kickoff & Planning | Week 1 | Scope validation, Rules of Engagement (ROE), documentation review, framework selection discussion, stakeholder alignment |
| Discovery & Access Setup | Weeks 2–3 | Stakeholder interviews (IT, Legal, Compliance), policy and artifact collection, access setup for systems, cloud, and apps |
| Compliance Assessment | Weeks 2–6 | Framework mapping (NIST CSF, 800-53/171, HIPAA, GDPR, ISO), maturity scoring, gap analysis, roadmap drafting |
| Penetration Testing | Weeks 3–6 | Internal/external testing, 3–5 web apps, wireless, Microsoft 365/Azure/SaaS security posture analysis |

| | | |
|----------------------------------|-------------|--|
| AI Governance & Security Audit | Weeks 4–6 | Policy review (AI usage, Copilot, GenAI tools), governance gap analysis, AI threat modeling (no model testing) |
| Purple Team Exercise | Weeks 6–9 | Threat simulations, blue team engagement, detection tuning, real-time coaching, post-exercise debrief |
| IT Governance & Risk Review | Weeks 6–9 | Risk roles, escalation workflows, DR/BCP, alignment to enterprise governance expectations |
| Privacy & Data Protection Review | Weeks 10–14 | Data classification schema (draft), access control audit, encryption standards, HIPAA/GDPR alignment |
| Retesting & Validation | Weeks 10–14 | Validate remediated vulnerabilities; update vulnerability status (Closed/Partial/Open); residual risk comments |
| Final Reporting & Board Briefing | Weeks 10–14 | Final executive/technical reports, risk register, compliance roadmap, in-person board presentation , optional Q&A session |

Note: Several workstreams (e.g., AI Security Audit, Privacy Review, Governance Review) will run concurrently to maximize delivery efficiency while reducing burden on SBCERA teams.

Staffing And Qualification

Symosis will assign a cross-functional team with deep expertise across cybersecurity compliance, offensive security, cloud/SaaS configuration, and AI governance. Each workstream will be led by certified professionals with public-sector experience and domain-specific specialization to ensure delivery excellence.

Our team structure ensures dedicated leadership across all core workstreams, while drawing upon broader Symosis expertise for emerging risks, automation, and policy development.

Core Team Roles & Credentials

| Role | Responsibilities | Certifications / Experience |
|--|---|--|
| Engagement Lead / Principal Consultant | Oversees all phases of engagement, ensures stakeholder alignment, leads executive reporting and board presentations | CISSP, CISA, MBA (Public Sector), 15+ years with CalPERS, State Bar of CA, KCERA |
| Compliance & GRC Lead | Manages framework alignment, risk register development, policy mapping, and roadmap design | ISO 27001 Lead Auditor, CISM, HIPAA/GDPR specialist |
| Penetration Testing Lead | Leads internal/external testing, web application testing, and Purple Team execution | OSCP, CEH, Burp Pro Advanced, PTES/MITRE specialist |
| Cloud & SaaS Security Engineer | Reviews Microsoft 365, Azure, and SaaS configurations; performs | CCSP, Azure Security Engineer, CIS Benchmarks contributor |

| | | |
|------------------------------------|--|---|
| | hardening assessments and SSPM analysis | |
| AI Governance & Automation Advisor | Reviews AI tool usage, policy alignment, and automation opportunities via ServiceNow or Power Automate | GenAI risk researcher, Power Platform certified, AI policy reviewer |
| Project Manager (PMO) | Tracks milestones, coordinates weekly updates, ensures on-time deliverables, manages change requests | PMP, Agile Scrum Master, 10+ years supporting public agency assessments |

Team Attributes

- **Public Sector Experience:** Engagements with pension systems, county governments, and state regulatory agencies
- **Cloud & SaaS Focus:** Specialized expertise in Microsoft 365, Azure AD, and 30+ SaaS tools (including Shadow IT and SSPM posture mapping)
- **AI Risk Advisory:** Thought leadership on GenAI adoption, governance enforcement, and emerging policy frameworks
- **Offensive Security Depth:** Real-world red team simulation experience across multi-cloud and hybrid environments

Bios & Staffing Flexibility

Brief bios of our proposed delivery team are included in **Appendix A: Personnel Bios**. Symosis maintains a deep bench of additional specialists and can augment the team based on the evolving needs or optional service expansions during the engagement.

Fixed Fee AND Core Service Scope

Symosis proposes a **fixed fee of \$96,000** for execution of the core cybersecurity assessment and advisory services described in this proposal. This engagement will be delivered over a **14–18 week period** and includes planning, execution, risk analysis, stakeholder reporting, and an **in-person presentation to the SBCERA Board**.

Included Core Service Areas

1. **Cybersecurity Compliance Assessment** (NIST CSF, NIST 800-53/171, ISO 27001, HIPAA, GDPR)
2. **External and Internal Penetration Testing** (up to 500 IP-based assets)
3. **Web Application Security Testing** (up to 5 applications; authenticated where applicable)
4. **Wireless Network Security Assessment** (at SBCERA's San Bernardino site)
5. **Cloud and SaaS Configuration Review** (Microsoft 365, Azure AD, and ~30 SaaS applications across ~35 accounts)
6. **AI Governance and Security Audit** (focused on SBCERA's adopted AI policy and GenAI tool usage)
7. **Purple Team Simulation Exercise** (threat simulation, detection testing, blue team coaching)

8. **Retesting of Remediated Findings** (validation of closure and updated risk ratings)
9. **IT Governance and Risk Management Review** (roles, escalation, policy maturity, DR/BCP)
10. **Data Protection and Privacy Review** (data classification, encryption, HIPAA/GDPR controls)

Fixed Fee Also Includes

- End-to-end **project management and resource coordination**
- **Weekly status calls and written updates**
- **Real-time escalation of critical findings**
- **Preliminary findings** prior to final reporting
- **Final technical reports** and summary documents for each domain
- **Executive Summary** with board-ready insights
- **In-person board presentation** at engagement conclusion
- **One post-engagement Q&A or leadership deep-dive session** (optional)

Optional Services (Future Phases or Add-Ons)

Symosis offers a full suite of optional services that may be delivered concurrently or in future phases based on SBCERA's priorities. These include:

- Security awareness training & phishing simulations (1–2/year)
- Incident response tabletop exercises
- Secure SDLC reviews and DevSecOps support
- AI workflow optimization and automation implementation (Power Automate, ServiceNow)
- SaaS security posture management (SSPM) and SaaS risk assessments
- Identity & access governance assessments
- Microsoft 365 / Azure hardening
- Custom threat simulations or tabletop designs
- Incident response playbook development
- Cybersecurity metrics & board dashboard development

These services will be scoped collaboratively and priced based on level of effort.

Blended Hourly Rate Schedule

| Role | Rate (USD) |
|-------------------------------------|-------------------|
| Symosis Project Team (Blended Rate) | \$165/hour |

Our blended rate includes a mix of principal consultants, engineers, and analysts. Optional work will only begin after mutual agreement on scope and estimated hours.

Conclusion

Symosis is uniquely positioned to support SBCERA in advancing its cybersecurity, compliance, and governance maturity. Our combination of deep technical capability,

experience with public retirement systems, and focus on risk-informed, practical execution ensures we will deliver lasting value throughout this engagement.

We understand the fiduciary importance of protecting sensitive data, sustaining trust with members and stakeholders, and aligning to evolving frameworks like NIST, HIPAA, and AI governance best practices. Our team is committed to delivering not just findings—but actionable, prioritized guidance, supported by executive-ready reporting and an in-person presentation to the SBCERA Board.

We appreciate the opportunity to submit this proposal and look forward to partnering with SBCERA to protect the integrity of your systems, operations, and member mission.

Please don't hesitate to contact us with any questions or to schedule a walkthrough of our proposed approach.

Appendix A: Staff Bios

The following team members represent Symosis' core delivery staff, each bringing deep experience in cybersecurity, compliance, penetration testing, AI security, and public-sector risk management. This roster reflects our ability to support SBCERA with both strategic insight and technical execution.

| Name & Title | Key Experience | Certifications & Education |
|---------------------------------|--|--|
| Kartik Trivedi, Partner | 20+ years leading cybersecurity strategy for Fortune 100s and public agencies. Former security engineer and program builder. | CISSP, CISA, CISM, C |
| Clinton Mugge, Partner | Ex-counterintelligence agent turned cyber strategist. 20+ years in cyber risk and governance for large enterprises. | CISSP MS – Univ. of Maryland, BS – Southern Illinois |
| Eric Tomasi, Partner | 25+ years in compliance leadership and interim CISO roles. Led programs across public and private sectors. | CISSP, C |
| Jeff Brock, Partner | Former head of Autodesk cloud security. Led FedRAMP and ISO certifications for global SaaS platforms. | CISSP, CISM BS Computer Science |
| Dave Patel, Sr. Manager | Vendor risk and GRC specialist. Deep experience with ISO/NIST frameworks and tooling. | CISSP BS Information Security |
| Sanskar Tewatia, AI/ML Engineer | ML expert focused on secure model design and AI-driven automation for cybersecurity use cases. | MS – Electrical & Computer Engineering (ML) |

| Name & Title | Key Experience | Certifications & Education |
|--|--|--|
| Pranav Saji, AI/ML Engineer | AI engineer with background in ML applications and automation in enterprise environments. | MS – Illinois Institute of Tech PG – Machine Learning & AI |
| Vatsal Sonecha, Partner | Ex-Synopsys, Tenable, VMware leader. Strategy, partnerships, and virtual CISO program leadership. | MBA, BS Engineering |
| Gregory Paik, Manager | Security architect with red team and vulnerability management expertise. | CISSP BS Information Technology |
| Chaitali Parmar, Principal | Privacy and risk expert specializing in ISO/NIST compliance, privacy audits, and data mapping. | CIPM BS Computer Science |
| Natalia Belaya, Principal | Former Autodesk ISO lead. 15+ years in cloud compliance, IT audit, and program management. | CISM, ISO 27001 BS Computer Engineering |
| Parth Bhawsar, Manager | Threat detection and incident response leader with strong SOC and IR background. | CISSP, CCNA MS Information Security |
| Sukhvir Saini, Network Engineer | Hybrid infrastructure and secure network design engineer with 15+ years of hands-on experience. | CISSP BS Network Engineering |
| Wolfgang von Stuermer, Consultant | 20+ years in ethical hacking and enterprise security architecture. Former global CISO and CTO. | Ethical Hacker MS Cybersecurity – NYU |
| Vibhuti Mahant, Security Engineer | Cloud security engineer with experience in Azure/AWS and identity governance. | CISA, CISM, AWS/Azure Certified BS Computer Science |
| Tinatini Sandroshvili, Sr. Engineer – Threat Intel | Threat intel specialist. Former Degreed engineer with experience in SOC2, ISO audits, and detection logic. | CEH, Security+, CySA+, CCNA CyberOps, AWS Cloud Practitioner |
| Lenin Aboagye, Security Engineer | Cloud and IoT security advisor. Former CISO and speaker on AI/IoT threat defense. | CISSP BA Computer Science & Math – Cardinal Stritch |

Appendix B:
Request for Qualifications Signature Page

(Continued Next Page)

Exhibit A: Page 48

APPENDIX B

Request for Qualification

Cybersecurity Assessment and Services

SIGNATURE PAGE

FIRM NAME: Symosis Security

ADDRESS: 1250 Borregas Ave, Sunnyvale, CA 94089

E-MAIL ADDRESS: kartik@symosis.com


TELEPHONE #: 213-248-1130

FACSIMILE #:

FEDERAL EMPLOYER IDENTIFICATION #: 83-0640758

CONTACT PERSON FOR FIRM: Kartik Trivedi

By signing this Signature Page, through the undersigned representative who has the authority to bind the Firm, and by submitting a Submission in response to this RFP, the Firm agrees to perform the services required by such RFP and to accept and comply with all requirements, specifications, terms and conditions of the RFP if selected. Firm further agrees to be bound by this Submission for a minimum of 12 months from the date the RFP was issued.

SIGNED BY: 

Name: Kartik Trivedi

Title: Partner

Date: May 27, 2025