LOGICALIS
Architects of Change

Guiding Your Organization Through a Measured Cybersecurity Journey

Overwatch Program Overview

The Overwatch program is designed to support organizations in establishing, enhancing, and maintaining a mature cybersecurity posture aligned with recognized industry frameworks such as NIST, CIS, and others. Whether compliance is mandated or pursued as a best practice, Overwatch offers a clear and structured path to security excellence—empowering organizations to protect critical assets, ensure regulatory compliance, and reduce cyber risk.

Overwatch follows a phased approach that aligns your cybersecurity goals with a selected framework and supports your team through assessment, remediation, and continuous improvement.

Three-Phase Approach to Cybersecurity Maturity

Phase 1: Benchmarking & Assessment

We begin by evaluating your current security posture to define your program's objectives. Through a rapid assessment, we measure your existing controls against the chosen compliance framework. The outcome includes:

- A gap analysis report
- A Plan of Action and Milestones (POAM)
- A tailored remediation roadmap

Phase 2: Remediation & Planning

This phase focuses on policy development, procedural refinement, and creation or update of the System Security Plan (SSP). We also prepare for long-term success by:

- Recommending a governance and management structure
- Mapping out a strategic journey aligned to the POAM
- Laying the groundwork for ongoing compliance and continuous improvement

Phase 3: Overwatch (Ongoing Compliance & Management)

We provide continuous oversight and proactive security support to maintain compliance and enhance maturity.

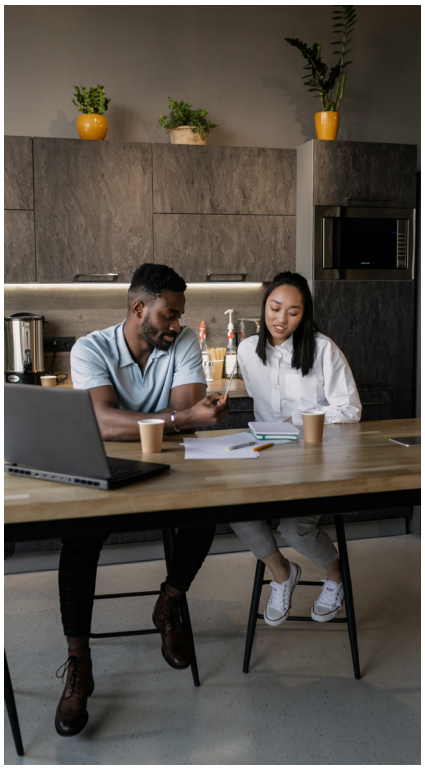
- Review of SIEM events and log sources
- Analysis of vulnerability scans, patch management, and high-risk items
- Firewall NAT rule and network segmentation reviews
- Physical and logical access control assessments
- Regular updates to POAM, asset inventories, and security roadmaps
- Supplier and product lifecycle evaluations
- Risk register and policy documentation updates
- Annual incident response documentation
- Business continuity and disaster recovery tabletop exercises

Key Benefits of Overwatch

Streamlined Audits: Leverage efficient tools and proven methods to reduce redundancy and simplify compliance efforts across multiple frameworks.

Framework Flexibility: Aligns with a wide range of standards and custom policies including NIST, CIS, ISO 27001, HIPAA, PCI, SOX, GDPR, DFARS, ITAR, Cyber Essentials, and others.

Expert Guidance: Access certified cybersecurity professionals (CISSP, CISM, RP) with deep industry knowledge and practical experience.



Why Overwatch Makes Business Sense

- **Resource Efficiency:** Offload time-consuming compliance tasks to a trusted partner so your internal team can stay focused on core operations.
- **Cost Optimization:** Avoid the high cost of maintaining a full-time compliance team (CISO, auditors, analysts, technical writers).
- **Reduced Friction:** Smooth the path to compliance through structured, well-managed processes that minimize disruption.
- **Regulatory Clarity:** Navigate the growing complexity of local and international security standards with confidence.
- **Risk Mitigation:** Ensure timely remediation and preparedness for audits to avoid fines, penalties, or reputational damage.
- **Insurance Readiness:** Meet the evolving demands of cyber insurers—compliance is increasingly required for obtaining or maintaining coverage.

LOGICALIS
Architects of Change