

Assignment 1.1: The Six Phases of the ADDIOI Model

Joshua A Wortz

University of San Diego

Course Number: CSOL-500

Dr. Michelle Moore

01/12/2024

Assignment 1.1: The Six Phases of the ADDIOI Model

Cybersecurity programs are critical for safeguarding an organization's assets and information. Schreider's (2020, pp. 26-27) Align, Design, Develop, Implement, Operate, Improve (ADDIOI) Model provides a structured six-phase approach to building such programs by aligning objectives with organizational goals, creating robust designs, implementing and operating countermeasures, and driving continuous improvement through performance metrics and maturity models. Schreider's seven design principles (2020, p. 31) enhance the effective implementation of cybersecurity measures by ensuring that critical business needs are not overlooked. Brown (2023) complements this framework by emphasizing risk-based prioritization, resilience, user-centric policies, adaptive defenses, holistic integration, data-driven metrics, and compliance with legal standards. Together, these frameworks ensure cybersecurity programs are robust, aligned with business priorities, adaptable to evolving threats, and grounded in best practices and governance. The principles outlined by Brown (2023), when applied within each phase of Schreider's ADDIOI Model and seven design principles, develop a comprehensive and continually improving cybersecurity program.

The first phase in the model, Align (Schreider, 2020, p. 26), focuses on identifying cybersecurity objectives and ensuring they connect with organizational goals. This phase provides the program support and drives the business requirements to offer help with executive buy-in. The align phase ties directly with the fifth design principle, "The cybersecurity program will be an enabler to the business aligning to stakeholder requirements" (Schreider, 2020, p. 31). As Brown has discussed, security programs will "stall or go nowhere" (2023 p. 7)

without knowing the business goals and needs. Therefore, it is imperative to identify key business processes and focus security programs around those processes, fulfilling the need to gain stakeholder buy-in and become a steadfast ally of the business.

The Design phase involves creating a blueprint for the cybersecurity program, incorporating frameworks, models, and a clear vision of the program's structure. The design phase aligns with the first and second principles from Schneider, which says that cybersecurity programs exist to protect assets and information and the cost of programs should be "commensurate with the value of those assets and information" (2020, p. 31). Using Schneider's (2020) insights, the program's blueprint must highlight measures to secure high-value assets and sensitive information, create a clear structure such as roles, responsibilities, and service management practices, and ensure robust program design while addressing business-specific risks. Focus on this portion is critical, as the job of cybersecurity experts is to advise on identifying and mitigating risks and creating a program that does not cost more than the value of the items targeted. Having a program that costs more than the value of the items targeted is poor business practice, as cybersecurity should not be cost-prohibitive.

Schneider's Develop phase configures and tests cybersecurity measures to meet design requirements (2020, p. 26). Activities include creating application integrations and hardening infrastructure. Incorporation of the sixth principle in this phase, which focuses on "real and likely threats" (Schneider, 2020, p. 31), ensures that only the most essential tools are in the program. As Brown (2023) discussed, risk-based assessments help prioritize countermeasures, ensuring the development of resources to mitigate the most pressing risks. For example,

integrating advanced endpoint protection tools and threat intelligence systems addresses current threat landscapes and gives protection, heuristics, and intelligent threat analysis on our edge. By testing and ensuring they are effective at meeting the design criteria while providing prioritized remediation and visibility, a team can be swift and responsive to future design changes.

The Implementation phase executes the plans and “goes live” with countermeasures, policies, and training programs (Schneider, 2020, p. 26). It can be one of the most sensitive moments, as security tools without proper implementation can affect business processes. It is essential to incorporate service management practices described in the third principle to ensure successful implementation (Schneider, 2020, p. 31). Through service management, critical processes such as organizing, training, and tools aid in instilling a security culture. For instance, providing security awareness training emphasizing phishing prevention creates a human firewall—an effective first line of defense against threats. Implementation is the most challenging phase, which can cause many security programs to fail. Rushing toward this phase will ultimately lead to losing trust in processes, tools, and teams.

The Operate phase oversees the cybersecurity program's day-to-day functioning, including SecOps, threat monitoring, and service desk operations (Schneider, 2020, p. 26). Using frameworks like ITIL for service management and aligning operations with ISO standards ensures program sustainability. Brown (2023) emphasizes operational efficiency's importance in adapting to evolving cybersecurity landscapes, which aligns with the seventh principle

(Schreider, 2020, p. 31). Operating is essential because the threat landscape grows and changes daily. The insights gained from operating will inform the next and final phase.

The cycle concludes with the Improve phase, where continuous improvement ensures the program evolves to meet changing needs and threats (Schreider, 2020, p. 26). This phase involves performance monitoring, assessments, and maturity model-based guidance. As detailed in the fourth principle, regular audits, key performance metrics, and adherence to legal requirements ensure the program remains effective and compliant. For example, Schreider (2020, p. 27) highlights using maturity models to create a performance baseline and drive program enhancements. Failing to continually improve and develop cybersecurity programs will ultimately lead to antiquated security controls that put organizations at risk because of constantly changing threat actors, laws, and regulations.

The ADDIOI model provides a systematic framework for designing and managing an effective cybersecurity program. By aligning each phase with the seven design principles, organizations can ensure their cybersecurity initiatives are robust, compliant, and adaptable to evolving threats. Insights from Schreider (2020) and Brown (2023) reinforce the importance of aligning cybersecurity strategies with business goals and leveraging good practices to achieve long-term success.

References

Brown, J. (2023). *Executive's Cybersecurity Program Handbook: A Comprehensive Guide to Building and Operationalizing a Complete Cybersecurity Program*. Packt Publishing, Limited.

Schreider, T. (2020). *Building an Effective Cybersecurity Program, 2nd Edition* (2nd ed.). Rothstein Publishing.