

Assessment Report

Framework: seal

Firm: ABC

Date: September 24, 2025

Prepared by SecureEngage

Executive Summary

ABC's current posture against the SEAL framework demonstrates a solid foundation in policy management and incident response testing. The firm has successfully met the requirements for SEAL-001, indicating that policies are reviewed annually and remain current. Additionally, ABC meets the criteria for SEAL-002, showcasing evidence of incident response testing that aligns with the SEAL methodology.

Key strengths include:

- Robust annual policy review process ensuring compliance and relevance.
- Effective incident response testing that enhances preparedness and resilience.

However, there are key gaps that need to be addressed to strengthen ABC's overall security posture. These include:

- Lack of comprehensive documentation on the outcomes of incident response tests.
- Insufficient training programs for staff on updated policies and incident response procedures.

By focusing on these areas for improvement, ABC can enhance its alignment with the SEAL framework and bolster its overall security effectiveness.

Governance and Risk Management

The Governance and Risk Management analysis for ABC firm reveals a strong adherence to established protocols and standards as outlined in the SEAL framework.

Key findings indicate that the firm is effectively managing its governance and risk processes. Specifically, the SEAL-001 policy review demonstrates that ABC consistently reviews its policies on an annual basis, ensuring that they remain current and relevant. This practice mitigates the risk of operating under outdated guidelines and reinforces the firm's commitment to compliance and best practices.

Additionally, the SEAL-002 incident response testing shows that ABC has implemented a robust incident response strategy. Evidence suggests that the testing aligns well with the SEAL methodology, indicating that the firm is prepared to respond to potential incidents effectively. This proactive approach not only enhances the firm's resilience but also builds confidence among stakeholders regarding its risk management capabilities.

In summary, ABC firm exhibits commendable governance and risk management practices, with key areas of policy review and incident response testing meeting the required standards. These findings reflect a solid foundation for ongoing risk management efforts and a commitment to maintaining high governance standards.

Cyber Security

The cyber security analysis for ABC firm indicates a positive compliance status with respect to the SEAL framework.

Key findings include:

- SEAL-001.policy_review: The firm meets the requirements, demonstrating that its security policies are reviewed annually and are not expired. This practice ensures that the policies remain relevant and

effective in addressing current threats and vulnerabilities.

- SEAL-002.ir_testing: The firm also meets this criterion, providing evidence of incident response testing that aligns with the SEAL methodology. This indicates that ABC is proactive in preparing for potential security incidents, ensuring that its response strategies are effective and well-practiced.

Overall, ABC firm shows a commitment to maintaining robust cyber security practices through regular policy reviews and effective incident response testing. These efforts contribute to a stronger security posture and better preparedness against cyber threats.

Recommendations

Based on the SEAL framework assessment for ABC, the following prioritized recommendations are provided:

1. ****Enhance Incident Response Training**** Rationale: While incident response testing is conducted, ongoing training for staff involved in incident response can improve readiness and effectiveness during actual incidents. This will ensure that all team members are familiar with their roles and responsibilities. Estimated Effort: Medium - This will require developing training materials and scheduling sessions, which may take 2-4 weeks.
2. ****Regular Policy Updates for Emerging Threats**** Rationale: Although policies are reviewed annually, it is crucial to ensure they are updated in response to emerging threats and changes in the regulatory landscape. This proactive approach will help maintain compliance and enhance security posture. Estimated Effort: Low - This can be integrated into the existing annual review process, requiring an additional 1-2 weeks for research and updates.
3. ****Conduct a Comprehensive Risk Assessment**** Rationale: A thorough risk assessment will identify vulnerabilities and areas for improvement beyond the current incident response capabilities. This will provide a clearer picture of the organization's risk landscape and inform future security initiatives. Estimated Effort: High - This process may take 4-6 weeks, involving multiple stakeholders and potentially external expertise.
4. ****Implement Continuous Monitoring Solutions**** Rationale: Continuous monitoring can help detect and respond to threats in real-time, enhancing the overall security posture. This aligns with best practices and can significantly reduce response times to incidents. Estimated Effort: High - Implementation may take 6-8 weeks, depending on the complexity of the systems and integration requirements.
5. ****Establish a Communication Plan for Incident Response**** Rationale: A well-defined communication plan will ensure that all stakeholders are informed during an incident, facilitating a coordinated response. This is essential for maintaining trust and transparency with clients and regulatory bodies. Estimated Effort: Medium - Developing the plan and conducting training may take 3-5 weeks.

By prioritizing these recommendations, ABC can strengthen its incident response capabilities, enhance policy effectiveness, and improve overall security resilience.

Third-Party and Outsourcing Oversight

The Third-Party & Outsourcing Oversight analysis for ABC has been conducted using the SEAL framework. The assessment focuses on the effectiveness of the firm's policies and incident response

capabilities in relation to third-party and outsourcing engagements.

Key findings from the analysis indicate that ABC demonstrates compliance with the SEAL framework in two critical areas:

- SEAL-001.policy_review: The firm meets the requirements, as there is clear evidence that policies are reviewed annually. This ensures that all guidelines remain relevant and up-to-date, mitigating risks associated with outdated procedures.
- SEAL-002.ir_testing: The firm also meets the criteria for incident response testing. Evidence shows that ABC conducts testing aligned with the SEAL methodology, which is essential for ensuring preparedness in the event of a security incident.

Overall, ABC exhibits a strong commitment to maintaining effective oversight of third-party and outsourcing relationships through regular policy reviews and robust incident response testing. This proactive approach contributes to the firm's resilience against potential risks associated with external partnerships.

Conclusion

In conclusion, the assessment of ABC against the SEAL framework has yielded positive results. The firm demonstrates a strong commitment to maintaining effective policies and incident response protocols.

Key findings include:

- SEAL-001.policy_review: The firm meets the requirement, with evidence indicating that policies are reviewed annually and remain current.
- SEAL-002.ir_testing: The firm also meets this requirement, as there is documented evidence of incident response testing that aligns with the SEAL methodology.

Overall, ABC has established a solid foundation in its policy management and incident response capabilities, reflecting a proactive approach to risk management and compliance. Further efforts to enhance these areas will continue to strengthen the firm's resilience against potential incidents.

Technology Operations and Resilience

The Technology Operations & Resilience analysis for ABC has been conducted using the SEAL framework, focusing on key operational policies and incident response capabilities.

Key findings indicate that ABC is effectively managing its technology operations and resilience through established practices.

The review of policies, designated as SEAL-001, demonstrates that ABC meets the required standards. There is clear evidence that policies are reviewed on an annual basis, ensuring they remain current and relevant. This proactive approach helps mitigate risks associated with outdated or ineffective policies.

In terms of incident response capabilities, SEAL-002 indicates that ABC also meets the necessary criteria. The firm has implemented incident response testing that aligns with the SEAL methodology. This testing is crucial for ensuring that the organization can respond effectively to potential incidents, thereby enhancing overall resilience.

In summary, ABC has established a solid foundation for technology operations and resilience, as evidenced by its adherence to policy review and incident response testing protocols. These practices contribute to the firm's ability to maintain operational integrity and respond to challenges effectively.

Maturity Assessment and Gap Summary

The maturity assessment for firm ABC has been conducted using the SEAL framework, focusing on key areas of policy review and incident response testing. The evaluation reveals that ABC demonstrates a solid level of maturity in these critical aspects of its operations.

In the area of policy review, ABC meets the requirements outlined in SEAL-001. There is clear evidence that the firm's policies are reviewed annually and are not expired, indicating a commitment to maintaining up-to-date and relevant guidelines that govern its operations.

Similarly, in the realm of incident response testing, ABC also meets the criteria set forth in SEAL-002. The firm has provided evidence of incident response testing that aligns with the SEAL methodology, showcasing its preparedness to effectively respond to potential incidents.

Overall, ABC exhibits a commendable level of maturity in the assessed areas. However, further assessments in additional SEAL categories may be necessary to identify any potential gaps and enhance the firm's overall resilience and operational effectiveness.

Key Findings Summary: - SEAL-001.policy_review: Meets - SEAL-002.ir_testing: Meets