RSA ARCHER® SUITE FOR THE U.S. DEPARTMENT OF DEFENSE

DIGITAL RISK IS MISSION RISK

The United States Department of Defense (DoD), like all federal agencies, is in the midst of modernization to support its mission and maintain competitive advantage for today's warfighters. As the battlefield and adversaries continue to evolve, the DoD also evolves to address new and emerging threats and manage operational, mission and digital risks. Digital modernization is driving change across the DoD enterprise to create a modern, secure, coordinated, transparent and cost-effective IT architecture that improves the cyber threat posture and transforms data into actionable information. Achieving this vision requires an integrated system and a consolidated view that effectively balances powerful data visualization with comprehensive risk and governance controls, based on open standards, the Risk Management Framework (RMF) and common taxonomies.

INTEGRATED RISK MANAGEMENT TO ADVANCE THE MISSION

The RSA Archer® Suite integrated risk management solution empowers the DoD to manage multiple dimensions of risk on one platform and quickly implement government and industry-standard processes and best practices for advanced risk management maturity, informed decision-making and enhanced mission performance. RSA Archer Suite's unified platform accelerates decision-making and enables DoD commands to consolidate data across the agency or department, using analytics to provide an integrated posture of risk and compliance activities. RSA Archer Suite addresses DoD modernization goals by prioritizing and promoting agile decision-making, increasing efficiencies, and ultimately, improving mission outcomes.

IT and security risk management helps improve decision-making by enabling DoD enterprise, departments and agencies to compile a complete picture of technology and cybersecurity-related risks and understand their mission and financial impacts.

Mission and operational risk management provides a clear, consolidated view of mission risk across the agency or department by aggregating disparate risk information in one central solution.

Third-party governance presents an accurate and complete picture of DoD third-party risk while also providing capabilities for managing and monitoring the performance of third-party relationships and engagements.

U.S. government-specific solutions enable agencies to improve information assurance programs and exceed FISMA and OMB requirements for continuous monitoring and assessment and authorization.

Mission resiliency automates mission continuity and disaster recovery planning and execution to protect DoD departments and agencies in the event of a crisis.

Compliance management consolidates information from multiple regulatory bodies to enable the DoD to establish a sustainable, repeatable and auditable compliance program.

Audit management transforms reactive, compliance-focused internal DoD audit function into a proactive, strategic enabler of the mission.

BENEFITS

- Provides executive dashboards for visibility into DoD cybersecurity risk management policies and practices

- Provides a common set of capabilities, methodologies and taxonomies for Risk Management Framework (RMF)

- Strengthens communication for agile decision-making across the DoD

- Enables information automation, risk analysis and metrics

- Offers flexible deployment— cloud or on-premises

- Simplifies management of NIST 800-53/171 and CMMC compliance

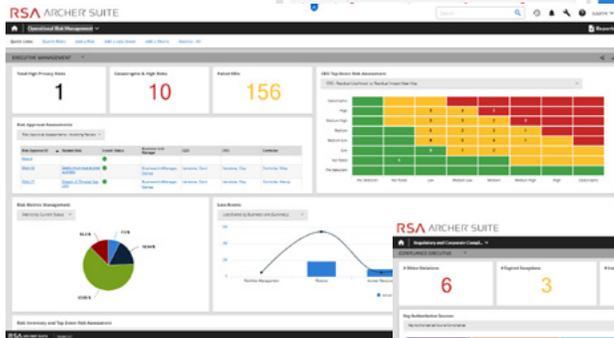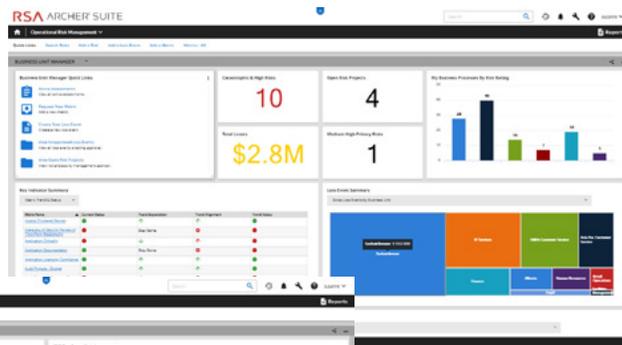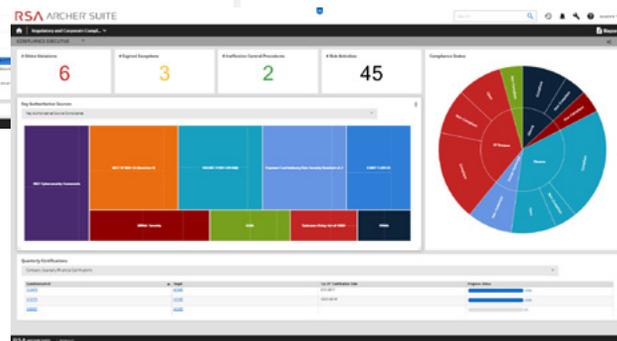*Figure 1: RSA Archer Suite executive dashboard example.*

Figure 2: RSA Archer Suite: single-pane-of glass visibility into operational, mission and compliance risks.

Digital modernization is driving change across the DoD enterprise to create a modern, secure, coordinated, transparent and cost-effective IT architecture that improves the cyber threat posture and transforms data into actionable information.

The RSA Archer Suite has been recognized as an industry leader. In fact, Dell Technologies (RSA) is a Leader in the 2019 Gartner Magic Quadrant reports for integrated risk management solutions, IT vendor risk management tools, IT risk management and business continuity management program solutions, worldwide. The RSA Archer Suite is also well established across government organizations for integrated risk manage. In fact, it is utilized in every branch of the U.S. government and many DoD agencies today.

CONCLUSION

RSA Archer Suite provides integrated risk management, empowering the DoD to make informed operational decisions:

• Quickly quantify mission risk with consolidated data and risk analytics

• Eliminate organizational silos and improve cyber threat posture

• Define and enforce accountability for a more agile and resilient defense posture

• Leverage process automation to optimize human and system efficiencies

Designed to help the DoD evolve its risk management program as requirements evolve, RSA Archer Suite includes preconfigured, easily tailorable, multidisciplinary mission-risk management solutions needed to cost-effectively address the most critical domains of enterprise risk.

ABOUT RSA ARCHER SUITE

RSA Archer® Suite enables organizations to manage the broad dimensions of business risk and confidently pursue digital opportunity. The suite is part of the RSA portfolio of business-driven security solutions, which provides a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change. For more information on RSA public sector solutions, go to rsa.com/publicsector