Tuesday, June 2

11:40 am– 12:00 pm

From Compliance Bottleneck to Continuous Readiness: AI-Driven ATO Automation with Integrated Risk, Security, and CORA Dashboards

Tom Bean

Advisory Solution Consultant, Risk

ServiceNow

Abstract:

The traditional ATO process was built for a slower era. Manual workflows, fragmented tools, and point-in-time assessments consume months of mission time while risk accumulates in the gaps between reviews. For most organizations, cybersecurity compliance runs as a separate discipline, disconnected from the enterprise IT systems, workflows, and data that actually reflect real risk posture. The result is an artifact-dependent process that lags reality by design.

For DoD organizations operating under persistent threat, that lag is unacceptable. Compliance latency is operational risk.

ServiceNow transforms ATO from a periodic administrative burden into a continuous, AI-accelerated mission capability. It does this from within the enterprise, embedding cyber risk management directly into the same platform that manages IT operations, service delivery, and infrastructure. Authorization evidence is generated by live operational data, not assembled after the fact.

When cybersecurity is integrated into the enterprise IT fabric, continuous authorization becomes achievable. AI continuously aggregates live operational data, tracks control status across the environment, and surfaces emerging risk, collapsing review cycles and enabling authorizing officials to make faster, better-informed decisions. ATO becomes a state of continuous preparedness, not a finish line organizations cross and then fall behind.

Commanders, ISSMs, and Authorizing Officials operate from real-time dashboards that translate live enterprise data into actionable risk intelligence. Because the platform

connects to the systems that run the organization, not periodic artifact submissions, the risk picture is current, not historical. Leadership sees a consolidated boundary-level view of posture scored against CORA readiness and JFHQ-DODIN priorities. When conditions change, the platform surfaces what is at risk and where to act first.

ServiceNow accelerates the process you already have, from inside your own enterprise. AI handles evidence aggregation, gap analysis, and remediation prioritization, freeing cybersecurity professionals to focus on mission-critical decisions rather than administrative overhead. Bringing cyber automation into your enterprise IT environment eliminates the handoffs, translation layers, and time delays that make traditional compliance unsustainable at operational tempo.

Integrated with eMASS, ACAS, STIG tooling, CMDB, and ITSM, ServiceNow serves as the AI orchestration layer that connects cyber risk management to the living enterprise. Existing investments are amplified. Evidence is derived from operational reality. Authorization posture reflects the environment as it actually exists, continuously.

Attendees will leave with a clear picture of how embedding AI-driven cyber automation within the enterprise shifts cyber readiness from a compliance exercise to a persistent operational advantage, enabling faster capability delivery and a stronger defensive posture across the DoDIN.