



How Konfer and Intel® power AI Safety and Assurance for the US Department of Defense

Learn how the US Department of Defense partnered with Konfer AI GRC and Intel® to develop an AI assurance capability for evaluating the safety of AI assets.



Introduction

Konfer AI GRC is a Governance-by-Design platform that focuses on AI Governance, Risk, and Compliance, accelerating enterprise AI innovation and adoption in compliance with global guidelines and regulations.

Powered by generative AI, Konfer converts policies and regulations to controls and creates a governance playbook; helps enterprises map all their AI assets (data, models, and applications); measures the assets' risk posture in real-time in accordance to the governance playbook, and assesses the conformance of these assets to AI and other statutory regulations.

AI GRC for Federal Government

AI governance is crucial for federal agencies to ensure adherence to regulations and guidelines, maintain public trust, and facilitate interagency coordination. It also helps manage large volumes of data responsibly, deliver public services equitably, and address national security concerns.

Konfer's AI GRC solution is well-suited to help government agencies comply with the various principles and requirements outlined in President Biden's Executive Order, especially in areas of safety, security, responsible innovation, and enhancing governance capacity.

The Challenge

The federal government handles highly sensitive and classified information. It has stringent policies against using third-party AI services such as Large Language Models for enterprise use cases due to significant security, compliance, and data privacy concerns. There are also concerns about the ethical use of AI, potential biases, and intellectual property issues.

These policies can impact platforms such as Konfer, which provides AI Governance using third-party Generative AI services, necessitating exploring opportunities and methods such as on-premise installation of all the components of the solution.

The Solution

1 On-premise AI solutions offer several advantages for federal agencies. They provide enhanced security by allowing full control over the infrastructure, minimizing the risk of data breaches and unauthorized access. Data privacy is ensured as agencies retain complete control over their data, which is crucial for handling classified information. Performance and reliability are improved with dedicated resources, reducing latency and ensuring higher uptime. Cost management becomes more predictable, with potential long-term savings compared to cloud service.

By utilizing Intel® hardware to set up on-premise infrastructure and running Intel® optimized Large Language Models on Intel® processors, Konfer can provide a platform that assures reliability of Intel® inside and AI GRC guard-railed by Intel® ecosystem.

2 Intel® powered Government Cloud, offered by popular cloud hosting platforms such as AWS and GCP. These are designed to host sensitive data, regulated workloads, and address the most stringent U.S. government security and compliance requirements such as FedRAMP High authorization to operate (ATO).

Konfer with Intel® Inside

Intel® offers a portfolio of AI solutions that provide competitive and compelling options to develop and run models such as Llama2-70b on-premise or in government cloud. Intel®'s rich hardware portfolio, combined with optimized open software, provides the perfect framework for Konfer platform to be compliant with stringent federal government policies around privacy and security.

Llama2-70b can run on Intel®'s AI portfolio that includes Habana Gaudi2 deep learning accelerator, 4th, 5th, 6th Gen Intel® Xeon® Scalable processors, Intel® Xeon® CPU Max Series, and Intel® Data Center GPU Max.

US Department of Defense Project: AI Safety and Assurance

Konfer is working with a US D.O.D. branch on a CRADA (Cooperative Research and Development Agreement) project on AI Safety and Assurance. The main objective of this CRADA is to develop and analyze an AI assurance capability that combines at least two approaches for evaluating the safety of AI assets. In the context of AI, assurance helps users understand if an AI asset is operating in a trustworthy, optimal, and risk-free way. The US D.O.D. branch is interested in two such publicly available approaches:

1 The first is an assurance case approach developed by the University of York called Assurance of Machine Learning for use in Autonomous Systems (AMLAS).

2 The second is a Naval Air Warfare Center Weapons Division adaptation of the U.S. Department of Defense Level of Rigor (LoR) approach specifically for AI.

While the approaches differ, each has guidance that could be helpful in developing an AI assurance capability for evaluating Government AI assets.

Konfer has completed a Proof-Of-Concept to prove the power of Intel® LLMs and Intel® hardware in solving the US D.O.D CRADA project of operationalizing the two AI/ML safety standards, specifically for the following three LLM use cases:

1 Setup and execute Controls Generation: Controls Generation is a generation of regulatory controls from the two AI/ML safety standards

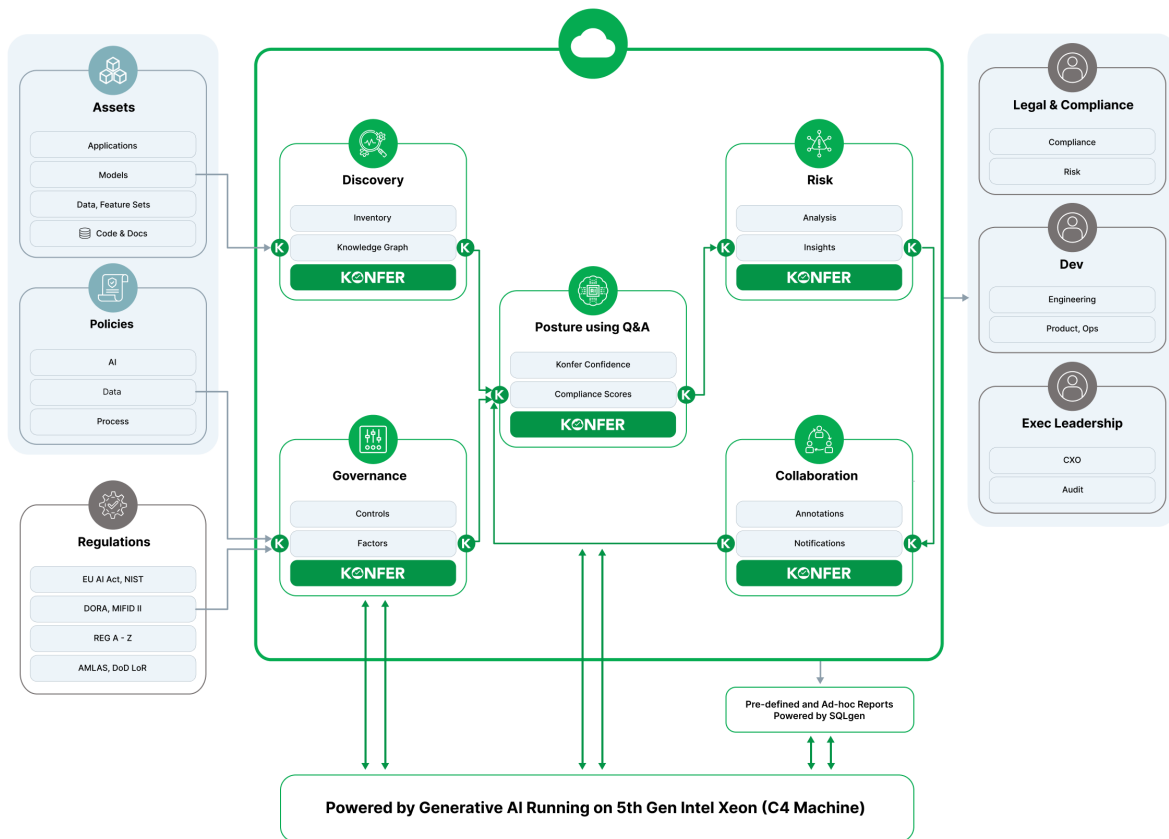
2 Setup and execute Questions & Answering: Answering the generated controls by matching the controls to AI/ML MDLC documentation from the US D.O.D. branch

3 Setup and execute SQL Generation: Natural language to SQL generation for user friendly compliance reporting

Results

Konfer, through the Proof-Of-Concept has identified a solution architecture that assures reliability of Intel® inside and the power of Konfer AI GRC guard-railed by the Intel ecosystem.

Konfer Instance running on Intel Xeon (Broadwell)



For the Proof-Of-Concept, Konfer utilized Intel® Emerald Rapids, also known as the 5th Generation Xeon, a server-grade processor designed for high-performance computing applications. It's typically installed on-premise in data centers or server rooms. The Large Language Model Llama2-70b was installed on the C4 machine series, which incorporates Intel® Advanced Matrix Extensions (AMX), a built-in accelerator and a higher memory capacity that enables low latency and parallel use cases.

Using Llama2-70b, Konfer was able to successfully set up and execute three key functions on the two approaches to evaluate AI assets' safety (AMLAS and the U.S. D.O.D. LoR): 1) Controls Generation, 2) Question and Answering, and 3) SQL Generation. These functions involved several intermediate steps, including controls rephrasing, source identification, ideal answer generation, asset type assignment, controls answering and snippet generation, all of which were effectively implemented in our Intel® powered framework. These comprehensive test runs ensure that AI assets are operating in a trustworthy, optimal, and risk-free way.

The Proof-Of-Concept proves the effectiveness of Konfer Governance-By-Design on AI asset safety assessments for the US D.O.D branch.

Next Steps

Konfer team will brand the instance as Powered by Intel® and work with Federal prospects to deploy this architecture. This involves qualified lead generation and future sale of the Konfer solution to US D.O.D. and Intelligence community using Intel® hardware and Intel® LLMs, which are critical components of this architecture.

Quotes from Leadership in this Project



“Through the successful demonstration of integrating Intel®-optimized LLMs into Konfer Playbook and Konfer Confidence, Konfer now has the capability to bring its powerful compliance solution to on-prem deployments in a secure, efficient, scalable and highly customizable manner.”

Dr. Baskar Jayaraman

CTO and Co-Founder Konfer



“The complexities of meeting regulatory requirements for AI compliance are challenging for enterprises, and they can become a barrier to achieving the full potential of their Gen-AI investments in a cost-efficient manner.

In collaborating with Konfer and their Agentic AI Compliance and Governance Platform, Intel® is proving that the value of Intel® AI accelerators and products, both Gaudi and x86 Xeon product line can address these challenges by enabling enterprises to deploy latest Gen AI solutions complying with evolving AI regulations while achieving a high performance and return of investment.”

Arijit Bandyopadhyay

CTO of Enterprise Analytics & AI
Head of Strategy Cloud and Enterprise CSV Group
Intel Corporation