

AI-Assisted Government Security Assurance

Client

The client is a national tax authority, responsible for collecting taxes, administering customs, and supporting critical government services. As part of its cloud modernization efforts, the organization evaluates enterprise technology platforms against the Baseline Informatiebeveiliging Overheid (BIO) — the Dutch Government Information Security Baseline. A global consulting firm was engaged to perform the security assessment, with Konfer providing AI-powered evidence analysis to accelerate it.

The Challenge

Government security assessments are fundamentally evidence-intensive. Before an enterprise platform can be approved for government use, assessors must confirm that hundreds of BIO-defined security controls have been adequately implemented and documented — reviewing extensive architecture documents, security manuals, operational procedures, certifications, and technical documentation across multiple vendors.

The work was almost entirely manual: consultants had to interpret regulatory intent, locate supporting evidence, determine whether it satisfied individual controls, identify gaps, and document conclusions. It consumed significant specialist effort, was difficult to scale across platforms, and often had to be repeated as products evolved. The consulting firm needed a way to dramatically cut the effort required for evidence analysis without compromising the rigor, explainability, and independence government assessments demand.

The Konfer Approach

The consulting firm engaged Konfer to augment — not replace — its security consultants, automating the most time-consuming portion of the BIO assessment: interpreting control requirements, analyzing vendor documentation at scale, locating supporting evidence, identifying documentation gaps, and producing explainable recommendations for expert review. The assessment covered four enterprise platforms from three major technology vendors:

- SAP Business Technology Platform (SAP BTP)
- SAP S/4HANA
- Red Hat OpenShift
- IBM Cloud Pak for Business Automation as a Service (CP4BAaaS)

The engagement remained fully document-based, with the consulting firm's consultants retaining final assessment authority.

Implementation

Konfer converted BIO v1.04vz — the baseline version in effect at the time — into structured security control obligations, then processed vendor technical documentation, architecture descriptions, security manuals, certifications, and operational guidance — automatically mapping documentation to individual BIO controls and identifying supporting evidence for each. Unsupported requirements and documentation gaps needing clarification were flagged directly. Every recommendation came with document references, rationale, and a confidence score, keeping AI output fully transparent and reviewable so it accelerated expert decision-making rather than replacing it.

Results

Instead of manually searching thousands of pages of documentation, the consulting firm's consultants received control-by-control evidence mapping, direct references to supporting documentation, clear identification of documentation gaps, and explainable recommendations ready for expert validation — on a methodology repeatable across products and frameworks as they evolve. The result was a more efficient, more consistent assessment process that preserved the independence and rigor government assurance requires.

Key Advantages

- Automated evidence mapping across thousands of pages of enterprise security documentation
- Faster government security assessments without compromising expert oversight
- Explainable recommendations with complete evidence traceability
- A repeatable methodology applicable across multiple technology platforms and security frameworks