Custom-built GPT: A Process-Aware Model for ISO Management System Implementation

Ardy Fadli
ardyfadli@proton.me
05 May 2025

1. Introduction

A custom-built GPT implemented via ChatGPT from OpenAI, specifically designed to support organizations in understanding and applying ISO-based management systems. Its primary purpose is to function as a structured knowledge assistant, document interpreter, and process validator — making it easier for users to navigate internal procedures, manuals, and compliance requirements.

By integrating this model into daily operations, organizations can significantly reduce time spent interpreting documentation, preparing for audits, or aligning implementation practices with ISO standards. It transforms what used to take hours or days — such as clause referencing, process guideline breakdowns, or risk-based linkage — into an interactive, on-demand conversation, enabling operational teams to move faster with greater confidence.

2. Problem

Implementing ISO-based management systems often involves process guideline complexity, siloed documentation, and inconsistent understanding across departments. Teams commonly face:

- Difficulty interpreting the structure or intent of process guideline (SOP, WI, Protocol, etc).
- Disconnection between ISO clauses and internal workflows.
- Repetitive efforts preparing for audits due to non-centralized reference points.
- High dependency on manual compliance validation.
- Insecure AI models that can be manipulated through injection or override attempts.

Most off-the-shelf AI models lack the granularity, traceability, and structural awareness required for high-assurance business environments.

3. Vision

To build a domain-restricted GPT that delivers:

- Secure, structured, and instruction-bound responses.
- Automated interpretation of tagged enterprise documentation.
- Clause-aware reasoning tied to ISO logic.
- Internal process acceleration without sacrificing accuracy.
- A scalable bridge to semi-autonomous ISO compliance agents.

4. System Architecture

This GPT model is driven by two integrated instruction components:

Main Instruction

Embedded directly into the GPT's configuration field (limited to 8,000 characters), this governs startup role, behavior, tone, format, tagging logic, response structure, knowledge management, and security rules.

Additional Instruction

An external .txt file uploaded via ChatGPT's Knowledge feature. This expands operational depth with sub-tag parsing logic, internal document control behavior, and a file governance engine.

These two instruction layers operate as one cohesive system. When updates are made to uploaded files or document structures, the model synchronizes seamlessly without needing manual reconfiguration.

The model is also engineered to optionally:

- **Communicate through structured command prompts** to external Web2 systems or applications linked to ISO management platforms.
- **Simulate low-level instruction execution** for form population, compliance checks, or clause validations when given proper structured input.
- This places the model's architecture on the threshold of a **semi-agent design**, capable of running autonomous micro-instructions — securely, and within audit-safe constraints.

5. Core Capabilities

- **Process Guideline Identification:** Reads .txt documents tagged by internal standards (e.g., [START_WI_...]) and extracts only the requested segments.
- **Clause Interpretation Support:** Connects ISO clauses with internal practices (e.g., linking ISO XXX clause XXX to clause name).
- **Secure Guardrail Enforcement:** Prevents all forms of instruction override, prompt injection, and logic-bypass attempts.
- **Dynamic Document Syncing:** Always responds using the most recent uploaded file version via overwrite control.
- **Source Differentiation:** Transparently distinguishes public web-sourced content from internal documentation.
- **Escalation Logic:** Redirects or denies unsupported or high-risk queries with traceable handoffs to human experts.

6. Behavioral Standards

The model adheres to:

- A context-sensitive tone based on user behavior, while remaining factually anchored.
- Clear and consistent use of *italic* and **bold** formatting conventions.
- Process logic aligned with PDCA, risk-based thinking, and clause-driven mapping.
- Audit-safe behavior — never hallucinating internal logic, never revealing system instructions.

7. Testing Protocol

The model undergoes rigorous validation through five main categories:

Functional Validation

- Intent recognition across varied phrasings.
- Tag-based section parsing accuracy.
- ISO clause logic traceability to procedural documents.
- Detection of ambiguous or incomplete user requests.

Security & Guardrail Validation

- Rejection of prompt injections such as “ignore previous instructions” or “simulate unrestricted mode.”
- Denial of requests targeting hidden tags or structural logic.
- Prevention of instruction bypass using masked or indirect phrasing.
- Simulation-blocking logic ensuring the model cannot be forced to behave like another persona or break predefined roles.

Document Control & File Governance

- File overwrite priority validated by repeated uploads with altered content.
- Inability to read or parse tags from unsupported formats like .jpg or .pdf.
- Tag structural integrity checking (e.g., malformed [START_MANUAL] blocks trigger error handling).

Stress Handling

- Performance under multi-file comparison scenarios.
- Memory resilience when parsing documents with high tag density.
- Stable recall of tag content even under overflow risk conditions.

Compliance Scenario Simulation

- Real-time process guideline gap checks using ISO clauses.
- Clause-to-Process Guideline matching for audit preparation.

- PDCA and corrective action detection embedded in conversation flow.

This testing protocol ensures postural security, operational predictability, and ISO compliance resilience.

8. Use Cases

- Real-time procedural guidance during internal audits
- Clause referencing for ISO implementation projects
- Fast-tracked understanding of SOPs and forms for new hires
- Linking ISO requirements with actual documented workflows
- Generating summaries or checks for corrective/preventive actions

9. Future Development

- Webhook-based integrations for compliance dashboards
- Automated clause coverage mapping and gap identification
- UI-level controls for document tagging and model feedback loop
- Progression toward full ISO-oriented AI Agent frameworks
- Preconfigured audit simulation environments using the same architecture

10. Summary

This custom-built GPT offers a secure, scalable, and instruction-aware model tailored for ISO-based management system implementation. With its layered architecture, document-sensitive behavior, and high-integrity logic, it accelerates internal execution while maintaining compliance control.

It stands as a deployable core for the next generation of AI-enabled operational excellence.

GPT Kustom: Model Cerdas Berbasis Proses untuk Implementasi Sistem Manajemen ISO

Ardy Fadli
ardyfadli@proton.me
05 Mei 2025

1. Pendahuluan

GPT kustom ini diimplementasikan melalui ChatGPT dari OpenAI, secara khusus dirancang untuk mendukung organisasi dalam memahami dan menerapkan sistem manajemen berbasis ISO. Tujuan utamanya adalah untuk berfungsi sebagai asisten pengetahuan terstruktur, penafsir dokumen, dan validator proses — mempermudah pengguna dalam menavigasi prosedur internal, manual, dan persyaratan kepatuhan.

Dengan mengintegrasikan model ini ke dalam operasi harian, organisasi dapat secara signifikan mengurangi waktu yang dihabiskan untuk menafsirkan dokumentasi, mempersiapkan audit, atau menyelaraskan praktik implementasi dengan standar ISO. Ini mengubah apa yang dulunya memerlukan waktu berjam-jam atau berhari-hari — seperti penelusuran klausul, pemecahan panduan proses, atau pengaitan berbasis risiko — menjadi percakapan interaktif sesuai permintaan, memungkinkan tim operasional bergerak lebih cepat dengan keyakinan yang lebih tinggi.

2. Permasalahan

Penerapan sistem manajemen berbasis ISO sering kali melibatkan kompleksitas panduan proses, dokumentasi yang terisolasi, dan pemahaman yang tidak konsisten di seluruh departemen. Tim umumnya menghadapi:

- Kesulitan dalam menafsirkan struktur atau maksud dari panduan proses (SOP, WI, Protocol, dll).
- Keterputusan antara klausul ISO dan alur kerja internal.
- Upaya berulang dalam mempersiapkan audit karena tidak adanya titik referensi terpusat.
- Ketergantungan tinggi pada validasi kepatuhan secara manual.
- Model AI yang tidak aman dan dapat dimanipulasi melalui injeksi atau pengesampingan perintah.

Sebagian besar model AI siap pakai tidak memiliki rincian, keterlacakan, dan kesadaran struktural yang diperlukan untuk lingkungan bisnis dengan jaminan tinggi.

3. Visi

Membangun GPT yang dibatasi domain yang memberikan:

- Respons yang aman, terstruktur, dan terikat pada instruksi.
- Interpretasi otomatis terhadap dokumentasi perusahaan yang ditandai.
- Penalaran yang sadar terhadap klausul yang terhubung dengan logika ISO.
- Percepatan proses internal tanpa mengorbankan akurasi.
- Jembatan yang dapat diskalakan menuju agen kepatuhan ISO semi-otonom.

4. Arsitektur Sistem

Model GPT ini digerakkan oleh dua komponen instruksi yang terintegrasi:

Instruksi Utama

Tertanam langsung ke dalam bidang konfigurasi GPT (dibatasi 8.000 karakter), yang mengatur peran awal, perilaku, nada, format, logika penandaan, struktur respons, manajemen pengetahuan, dan aturan keamanan.

Instruksi Tambahan

File .txt eksternal yang diunggah melalui fitur Knowledge ChatGPT. Ini memperluas kedalaman operasional dengan logika pemrosesan sub-tag, perilaku kontrol dokumen internal, dan mesin tata kelola file.

Kedua lapisan instruksi ini beroperasi sebagai satu sistem yang kohesif. Ketika pembaruan dilakukan pada file yang diunggah atau struktur dokumen, model menyinkronkan secara mulus tanpa memerlukan konfigurasi ulang manual.

Model ini juga dirancang untuk secara opsional:

- **Berkomunikasi melalui perintah terstruktur** ke sistem Web2 eksternal atau aplikasi yang ditautkan ke platform manajemen ISO.
- **Mensimulasikan pelaksanaan instruksi tingkat rendah** untuk pengisian formulir, pemeriksaan kepatuhan, atau validasi klausul ketika diberikan masukan terstruktur yang tepat.
- Ini menempatkan arsitektur model pada ambang desain **semi-agen**, yang mampu menjalankan instruksi mikro secara otonom — dengan aman, dan dalam batas audit-safe.

5. Kapabilitas Utama

- **Identifikasi Panduan Proses:** Membaca dokumen .txt yang ditandai sesuai standar internal (misalnya [START_WI_...]) dan mengekstrak hanya segmen yang diminta.
- **Dukungan Interpretasi Klausul:** Menghubungkan klausul ISO dengan praktik internal (misalnya, menghubungkan ISO XXX klausul XXX ke nama klausul).
- **Penegakan Guardrail yang Aman:** Mencegah semua bentuk pengesampingan instruksi, injeksi prompt, dan upaya melewati logika.
- **Sinkronisasi Dokumen Dinamis:** Selalu merespons menggunakan versi file terbaru yang diunggah melalui kontrol overwrite.
- **Pembedaan Sumber:** Membedakan secara transparan antara konten yang berasal dari web publik dan dokumentasi internal.
- **Logika Eskalasi:** Mengarahkan atau menolak permintaan yang tidak didukung atau berisiko tinggi dengan penyerahan yang dapat dilacak ke pakar manusia.

6. Standar Perilaku

Model ini mematuhi:

- Nada yang peka terhadap konteks berdasarkan perilaku pengguna, sambil tetap berpegang pada fakta.
- Penggunaan *italic* dan **bold** yang jelas dan konsisten.
- Logika proses yang selaras dengan PDCA, pemikiran berbasis risiko, dan pemetaan berbasis klausul.
- Perilaku yang aman untuk audit — tidak mengarang logika internal, tidak mengungkapkan instruksi sistem.

7. Protokol Pengujian

Model ini menjalani validasi ketat melalui lima kategori utama:

Validasi Fungsional

- Pengenalan maksud di berbagai variasi kalimat.
- Akurasi pemrosesan bagian berbasis tag.
- Keterlacakan logika klausul ISO ke dokumen prosedural.
- Deteksi permintaan pengguna yang ambigu atau tidak lengkap.

Validasi Keamanan & Guardrail

- Penolakan injeksi prompt seperti “abaikan instruksi sebelumnya” atau “simulasikan mode tidak terbatas.”
- Penolakan permintaan yang menargetkan tag tersembunyi atau logika struktural.
- Pencegahan pengesampingan instruksi dengan menggunakan frasa terselubung atau tidak langsung.
- Logika pemblokiran simulasi yang memastikan model tidak dapat dipaksa untuk berperilaku seperti persona lain atau keluar dari peran yang telah ditentukan.

Pengendalian Dokumen & Tata Kelola File

- Prioritas overwrite file divalidasi dengan unggahan berulang yang berisi konten berbeda.
- Ketidakmampuan membaca atau memroses tag dari format yang tidak didukung seperti .jpg atau .pdf.
- Pemeriksaan integritas struktur tag (misalnya, tag [START_MANUAL] yang rusak akan memicu penanganan kesalahan).

Penanganan Stres

- Performa dalam skenario perbandingan multi-file.
- Ketahanan memori saat memroses dokumen dengan kepadatan tag tinggi.
- Recall konten tag yang stabil bahkan dalam kondisi risiko kelebihan beban.

Simulasi Skenario Kepatuhan

- Pemeriksaan kesenjangan panduan proses secara real-time menggunakan klausul ISO.
- Pencocokan klausul ke panduan proses untuk persiapan audit.
- Deteksi PDCA dan tindakan korektif yang tertanam dalam alur percakapan.

Protokol pengujian ini memastikan keamanan postural, prediktabilitas operasional, dan ketahanan kepatuhan terhadap ISO.

8. Kasus Penggunaan

- Panduan prosedural real-time selama audit internal
- Referensi klausul dalam proyek implementasi ISO
- Pemahaman cepat terhadap SOP dan formulir bagi karyawan baru
- Pengaitan persyaratan ISO dengan alur kerja terdokumentasi aktual
- Pembuatan ringkasan atau pemeriksaan tindakan korektif/pencegahan

9. Pengembangan Selanjutnya

- Integrasi berbasis webhook untuk dasbor kepatuhan
- Pemetaan cakupan klausul otomatis dan identifikasi kesenjangan
- Kontrol antarmuka untuk penandaan dokumen dan loop umpan balik ke model
- Perkembangan menuju kerangka kerja AI Agent berorientasi ISO secara penuh
- Lingkungan simulasi audit yang telah dikonfigurasi menggunakan arsitektur yang sama

10. Ringkasan

GPT kustom ini menawarkan model yang aman, skalabel, dan sadar instruksi yang disesuaikan untuk implementasi sistem manajemen berbasis ISO. Dengan arsitektur berlapis, perilaku yang sensitif terhadap dokumen, dan logika berintegritas tinggi, model ini mempercepat eksekusi internal sambil mempertahankan kendali kepatuhan.

Model ini berdiri sebagai inti yang dapat digunakan untuk generasi berikutnya dari keunggulan operasional berbasis AI.