

Introduction

AI for IA

Abridged



WELCOME

We will start at 9.00am

Disclaimer:

This presentation and its contents have been developed, and are intended, for the use of those attending a workshop presentation by Stephen Foster in AI for IA as part of Slovenia IIA Training programme for IIA Slovenia 4th March 2026

This presentation has been prepared solely for educational and illustrative purposes. Whilst every effort has been made to ensure the factual accuracy of the content herein, no representation or warranty is given as to its accuracy. The material is not intended to give definitive answers to specific circumstances and as such is only intended to be used as a guide. It is recommended to seek independent expert advice relating to any specific situation. Stephen Foster and Generative Audit disclaims all warranties, expressed or implied, with respect to the contents of this material, including any warranties of accuracy, merchantability or fitness for a particular purpose. Nothing herein should be construed as legal advice.

This presentation should not be relied upon as the basis for making any investment or other decision and it is not claimed that any of the content or views contained herein, whether expressly made or implied, represents the views of management.

Use cases and prompt examples presented in the training are for illustrative purposes only, created in test environments with simplified fictitious data. They should not be relied upon for use in execution or tasks and other work, private or business related. Prompting techniques are not a guarantee of accuracy or veracity of output. You should always seek expert technical and legal advice before processing data in any tools or environments, if available you must always follow your organisations use policies. Use cases and example prompts will generate different results each time they are used in different models and environments, LLM models make mistakes, you must check the results and follow the advice of the model provider. The HITL is essential. Whilst care is taken to protect systems from electronic virus attack or other harmful event, no warranty is given that text or files shared during this training is free of any virus or other harmful matter and accepts no responsibility for any loss or damage resulting from the recipient receiving, opening or using it. Tools and features, connections, skills, coding, agents etc can introduce security risks, you should seek technical expert advice and understand such threats before use.

No liability is assumed for errors or omissions in the presentation. Links to other websites are used at the users own risk. The speed of technological change in this field is such that content may come out of date in relatively short time periods.

This presentation and its contents are wholly confidential and may not be further distributed or passed on to any other person or published, circulated or reproduced, uploaded, in whole or in part, by any medium or in any form for any purpose including as use of knowledge or training in LLM models and Generative AI technology without the written permission of Stephen Foster.

© 2024, 2025 Stephen Foster. All rights reserved. Unless otherwise stated. Some graphics and images are produced based on ideas of Stephen Foster and the generative capabilities on LLM Models. The Generative Audit brand name and the Generative Audit logo are the property of Stephen Foster and subject to copyright protection.

House Rules

- Please keep your cameras on. Place microphones on mute when not speaking.
- Recording of session is not permitted.
- We will pause for questions and exchange, but if you want to ask as we go along you are encouraged to do so.
- The course can finish early, or we run out of time depending on interaction. We may have to be ‘agile’ with some content.
- This is a new and emerging topic, we have people with varying experience and knowledge, for some it will be at a good level, for some too high and for some too low!

AI Hygiene for the Course

- **My basic hygiene rules :**

- Do not include in your prompt's information; or uploaded files any:
 - Personal Identifiable Information,
 - Confidential, Private or commercially sensitive information relating to any individual or business.
 - Anything you do not want others to see or know about you.
- I always de-activate allowing training for others.
- Information and prompts we provide and use contain fictitious companies, individuals and context.
- Examples and exercises are for training purposes only they are not to be treated as working templates and tools for operational use.
- Tools, models, features, links, files, prompts etc are used at your own risk.
- *Any Questions?*

Agenda

1. (Current) Limitations of Generative AI
2. Role of IA regarding AI
3. The internal auditors AI readiness checklist
4. Prompt Engineering Concepts & Strategies (Brief form)
5. A few Use Cases (if time permits)

Setting Expectations

- This is a course attempts to balance the strengths and weaknesses of the topic. It is an abridged version of a much longer course.
- The need for engagement and the need for scepticism and control.
- It is a very high-level introduction to some aspects of technology - each topic can be explored in much greater depth (we run 3 and 4 day classes), and many more topics could be covered.
- You will not be a Generative AI expert after this , that takes time, and engagement, and much deeper learning.
- We are only scratching the surface! We are not covering governance, legislation, required security etc.

SESSION 1

Current Limitations of Generative AI

What is Generative AI?

.... Any volunteers?

Generative Artificial Intelligence



- **Different** from what we have been largely used to – does not follow predetermined rules for its output. It’s not a calculator!
- **Generates “new”^{*} content** in the form of text, audio, video, code, images.
- Still a **narrow or weak** form of AI.
- To get the best out it, you should **understand it’s strengths & weaknesses!**

“It comes in a lot of different flavours”

* The “new” content resembles what it was trained on!

Critical Thinking* is essential when engaging with AI

It's Convincing!

It's Flattering!

It's over-confident!

It can "Hallucinate"

It can write with such authority and seeming reference to fact!

Will tell you it's a great point, agree with, won't say no. Eager to please!

It doesn't know what it doesn't know unless you push it to admit it.

It can make mistakes and "create" answers Just like a human!

The use of natural language as the interface tricks your brain!

Anthropomorphism! But it has no intent or conscience.

Always remember it's a prediction engine based on code and statistics!

* **Professional skepticism (GIAS 4.3)** – Inquisitiveness, critically assessing the reliability of information.

It Can Amaze You!

Insights & Ideas!

Creativity!

Productivity!

Makes Curiosity Easier!

It can see things you may not, and clear mental road blocks!

Multi media capabilities – text, images, code, audio: Unleash your imagination!

It does the things you don't like doing and that take a lot of time!

The deep research and advanced reasoning capabilities are surprising!

... it may and possibly will do more! Amara's Law.

Knowing when to reach for it

- **The dilemma:** You need to use it to learn when not to use it, and that requires some upfront investment and planning.

Examples of when it is not the right choice or people choose to abstain.

Policy prohibits use, or the lack of policy creates confusion.

It's probabilistic nature is not suited to the task eg. Large Data Set analytics are better suited to analytic tools with different AI capabilities

You simply don't have the time for the mistakes it may make.
(that's why we need tested, repeatable workflows and tools)

Learning point: Just giving access to tools and thinking everyone will get on with it is not adopting AI
We need a vision, a strategy and a plan.

Two Types of System

Deterministic

- **Same input = same output**
 - Guaranteed, reproducible results
- **Examples:**
 - Spreadsheet formula
 - Database query
 - Traditional software

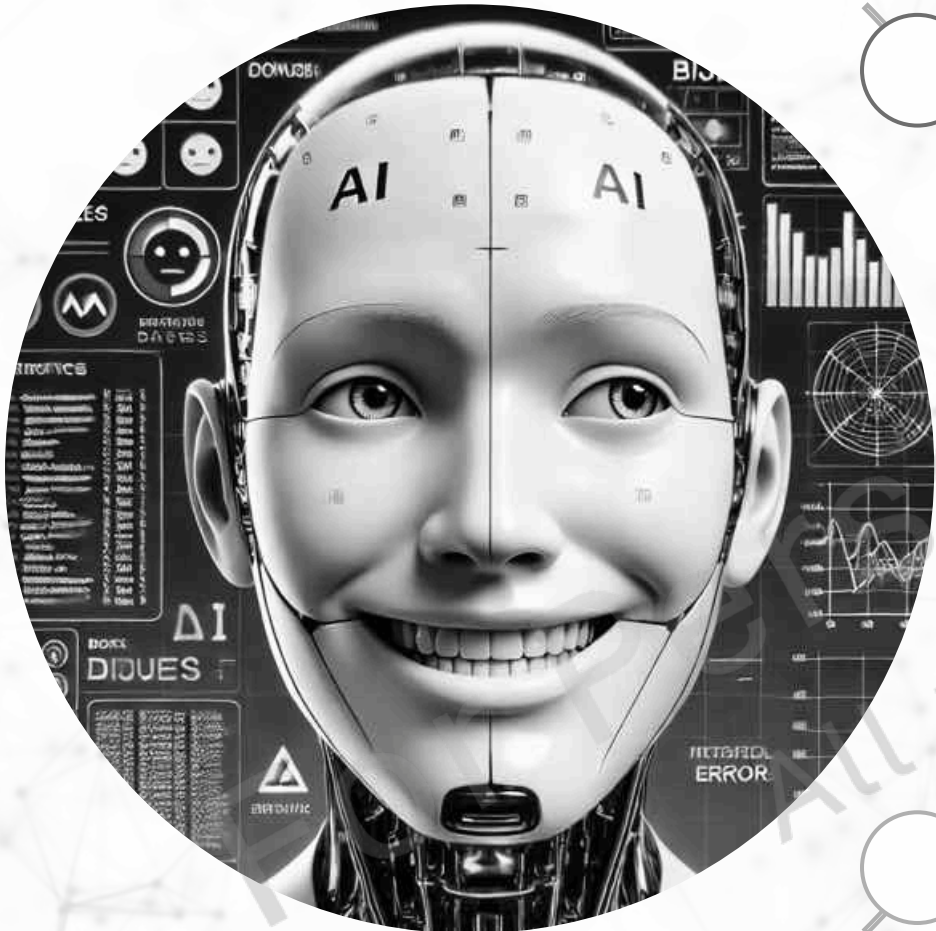
Probabilistic

- **Same input = variable output**
 - System calculates probability distributions
 - Each run draws differently from that distribution
- **Run it multiple times:**
 - Get variations

Where does AI sit , and specifically Generative AI?



Limitations: Forewarned is forearmed!



- **PREDICTION** based on training not a “library” knowledge.
- Limited **CONTEXTUAL** awareness.
- Correlation is not **CAUSATION**. Probability is not fact.
- They think “**INSIDE** the box”
- Cannot make **JUDGEMENTS**
- The sins of the father ... inherited **BIASES**
- Only as good as the **DATA** they are trained with.

Always remember

- Generative AI models **do not have any verification check, they do not understand if it is true or false.**
- **Responses** to prompts are **NOT pre-planned** or structured – they are **built token (word) by token**, one new prediction after another.
- There is no **“library of knowledge”** they call on.
- They **make predictions based on learned patterns and relationships** and apply probabilities.
- **“Hallucinations”** are not a bug as such, they are a **feature of probabilistic nature of the model.**

So where does this leave us?

Are we lovers or haters?

Will it bring a new Utopia for mankind?

Is this the beginning of the Matrix?

We don't know yet! Is it something in the middle?

- *It's certainly capable, but we must remain cautious and risk aware.*
 - *Yes - there are real limitations, but also real value!*
 - *Having a critical mind means we should be able to hold uncertainty with intellectual honesty, rather than a false confidence in either direction.*
- *The conclusion: **We Cannot Ignore It! We need to bring balance to the discussion!***

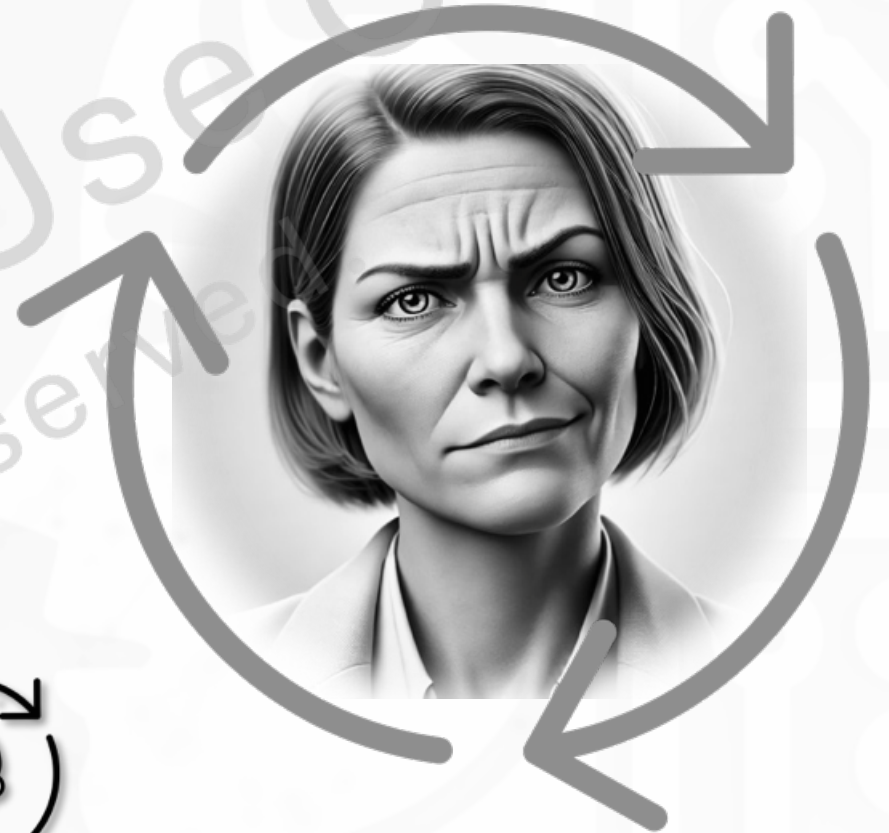


Is it OK to love and hate AI at the same time?

..... Absolutely, it may be critical!

A Critical Mind is fundamental to AI Use

- Our natural, objective, critical mind is our professions greatest asset!
- The **A**uditor **I**n **T**he **L**oop
 - **Professional scepticism** (GIAS 4.3) – Inquisitiveness, critically assessing the reliability of information.
 - Seek additional evidence to make a judgement.
- Important in every “chat” but also, a required control in all legislation and frameworks**.

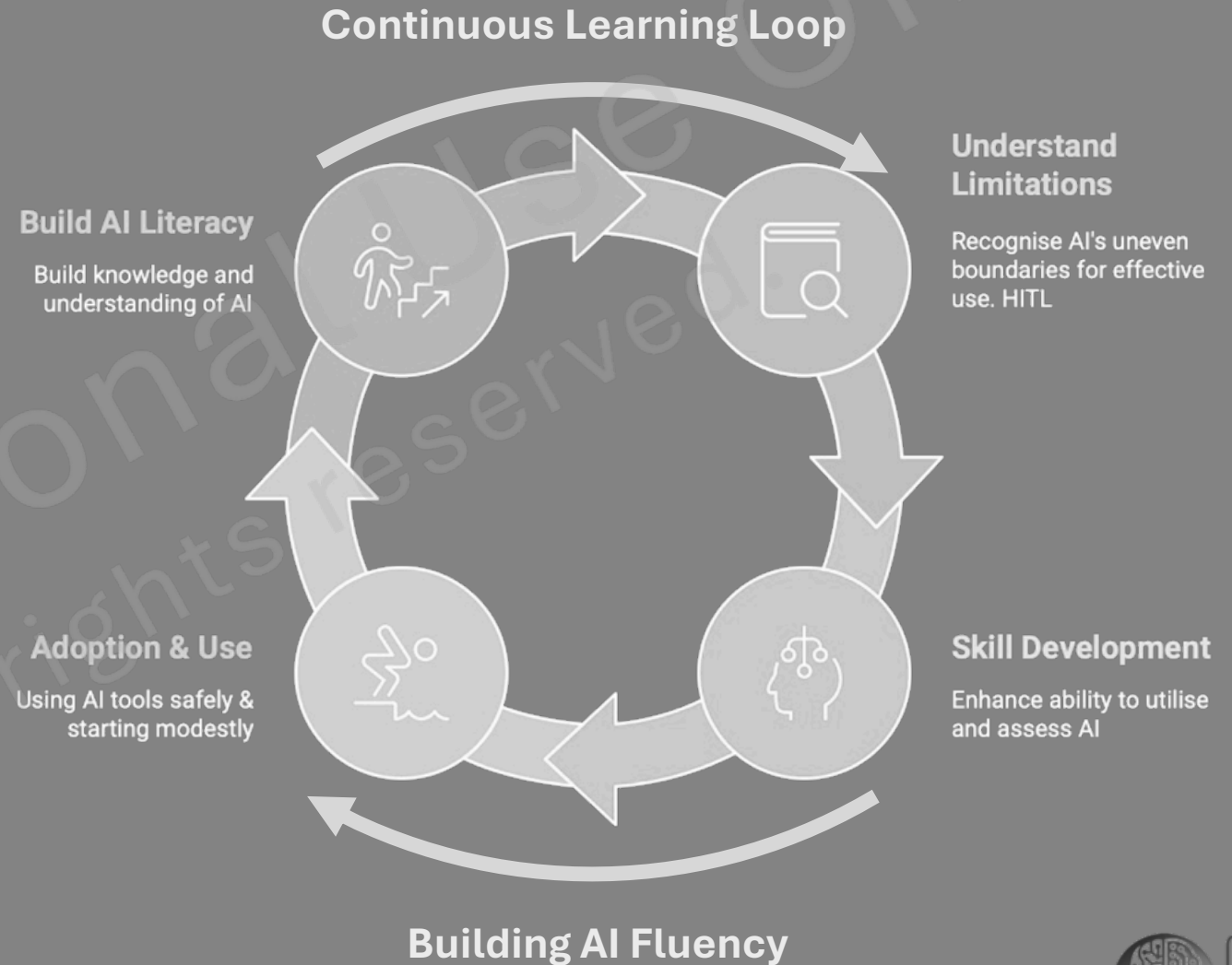


**

- Fundamental principle of Responsible AI
- Regulatory & Legislative Requirements: EU AI Act, GDPR art 22, US State Laws, US Exec Order etc
- Standards and Frameworks: ISO/IEC, NIST AI RMF, IEEE

Learning Cycle for Internal Auditors

- Ignoring AI is a higher risk than engaging!
- AI Literacy = core education, but always evolving
- Fundamental professional skill set for all.
- EU AI Act requirement.
- **Early , Safe use. Understand risks and needed controls.**
- **Use to build AI Fluency: Experiment, build, learn.**
 - Evolve and grow in sophistication of use.
 - Ability to creatively apply AI to solve problems, innovate, and create new value.
 - AI will never be “done” – evolving too rapidly, a continuous learning and development journey.



SESSION 2

The Role of Internal Audit

Internal Audits relationship with Generative AI

INTERNAL AUDIT & ARTIFICIAL INTELLIGENCE

USER

Efficiency & Quality
Impact & Insights

AUDITOR

Audit, Compliance, Risk Management
Ethical and Responsible use, doing what
it should, safely!

CHAMPION

Engaging Organisation
Balance
Leading by Example

Standards and Code of Practice: The User

- **Chartered IIA Code of Practice (2024):**

- **Resources** , Principle 28

- The chief audit executive should ensure that internal audit has the appropriate tools and technology to support the function's impact and effectiveness e.g. use of data analytics and **artificial intelligence**. Tools and technology should be used in internal audit activities, including to help auditors, analyse the risk profile to support scoping decisions, test controls and enhance internal audit coverage and quality. The function should regularly evaluate how tools and technology can be used to improve its effectiveness and efficiency.

- **IIA GIAS**

- **S 4.2 Due Professional Care:**

IAs must exercise due professional care by assessing the nature, circumstances, and requirements of the services to be provided, including:

- *[Removed]*
- **Use of appropriate techniques, tools and technology**

- **S 10.3 Technological Resources -The CAE Must:**

- Strive to ensure that the internal audit function has technology to support the internal audit process.
- **Regularly evaluate the technology used by the internal audit function and pursue opportunities to improve effectiveness and efficiency.**

When implementing new technology, the CAE must implement appropriate training for internal auditors in the effective use of technological resources. The CAE must collaborate with the organization's information technology and information security functions to implement technological resources promptly.

- **Communicate the impact of technology limitations on the effectiveness or efficiency of the internal audit function to the board and SM.**

GIAS: The Auditor

9.4 Internal Audit Plan

The CAE must:

- a) Create an internal plan that support the achievement of the organizations objectives;
- b) Base the internal audit plan on a documented assessment of the organization's strategies, objectives, and risks. This assessment must be informed by input from the board and SM as well as the CAEs understanding of the organisation's governance, risk management, and control processes. The assessment must be performed at least annually.

The internal audit plan must:

- Consider the internal audit mandate and the full range of agreed-to internal services.
 - Specify internal audit services that support the evaluation and improvement of the organization's governance, risk management, and control processes.
 - **Consider coverage of information technology governance**, fraud risk, the effectiveness of the organization's compliance and ethics programs, and other high-risk areas.
 - Identify the necessary human, financial, and technological resources necessary to complete the plan.
 - Be dynamic and updated timely in response to changes in the organization's business, risks operations, programs, systems, controls, and organizational culture.
- c) Review and revise the internal audit plan as necessary and communicate timely to the board and SM:
 - The impact of any resource limitations on internal audit coverage.
 - The rationale for not including an assurance engagement in a high-risk area or activity in the plan.
 - Conflicting demands for services between major stakeholders, such as high-priority requests based on emerging risks and requests to replace planned assurance engagements with advisory engagements.
 - Limitations on scope or restrictions on access to information.
 - d) Discuss the internal audit plan, including significant interim changes, with the board and SM. The plan and significant changes to the plan must be approved by the board.

IIA's: Artificial Intelligence Auditing Framework 2024

A guide to the first steps and approach to auditing an organisations approach and use of AI (ie. not auditing the models)

<https://www.theiia.org/en/content/tools/professional/2023/the-iias-updated-ai-auditing-framework/>



Guidance



Getting Started

Research & Info Gathering
Conversations and Engagement
Focus on Fundamentals



AI Auditing Framework

3 Domains

- Governance
- Management
- Internal Audits Role



Practitioner's Guide & Glossary

SESSION 3

Internal Auditors Readiness Check List for AI Use

Generative Audits Risk Taxonomy: Overview

① Data Risks

Bias, quality, poisoning, leakage, privacy, sovereignty, surveillance. Data risks are foundational — flawed inputs produce flawed models.

② Model Risks

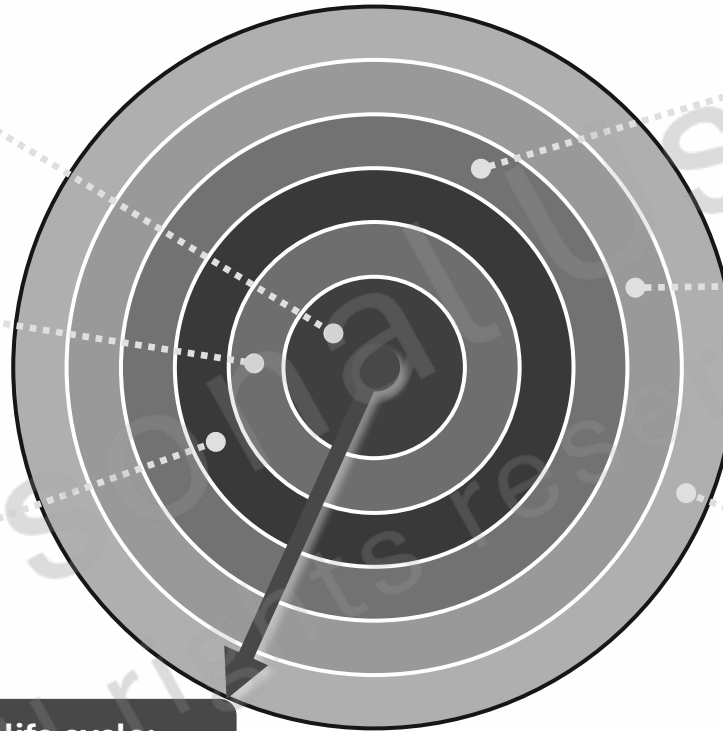
Hallucination, drift, explainability, algorithmic bias, robustness. Models can be confidently wrong, opaque and unstable over time.

③ Operational Risks

Shadow AI, automation bias, vendor and supply chain risk, skills gaps, prompt injection, cyber vulnerabilities, systemic failure.

Risks propagate through the life cycle:

Some risks originate in early stages of the life-cycle and cascade outward. Data and model risks propagate through operations, ethics, governance and beyond the organisation's boundaries. How the models are used in operations reverberates through the outer layers.



④ Ethical Risks

Discrimination, accountability gaps, autonomous decision-making, disintermediation, AI-enabled fraud and manipulation.

⑤ Strategic, Governance & Regulatory Risks

Regulatory non-compliance, regulatory lag, reputational risk, intellectual property uncertainty, governance failure.

⑥ Societal & Environmental Risks

Environmental impact, job displacement, cognitive enfeeblement, inequality in technology distribution, erosion of trust, large-scale AI harm.

There is not yet a single common risk topology or taxonomy, however there is very much a commonality of themes. (See COSO, MIT and NIST risk repositories in various links in the deck)

Safety Considerations include

(For illustration and discussion not decisions!)

Clear Guidance

- Essential -Can & Can't Do!
- AI Policy
- AI Literacy and Fluency Development
- Principles – Ethical , responsible transparent

Safety & Security

- Follow Organisation Policy and technical solution. Follow laws such as GDPR, EU AI Acts, sector regs & playbooks.
- Avoid/ Mitigate with Hygienic Prompts – structure inputs to avoid data disclosure
- Free models offer lowest levels of control over processing of data.
- Commercial Subscription may offer more control, but still a no to PII and Confidential info. etc
- Enterprise Models offer better options in configurations, infrastructure and SLA – **BUT always** an Organisation /IT decision and solution, don't assume.
- Data Sovereignty is amongst many data considerations needed.
- Air-gapped technologies, smaller scale models running on isolated computers are options to also consider.

Safety Considerations

Engage with your security team or IM teams, push for solutions (its worth it) and guidance, as many parties are working through these issues, establishing safes spaces with the right environment, mitigation and appetite.

... and don't forget, you can use AI beneficially without sharing anything confidential!

If in doubt, there is no doubt Don't!

Threats

ENTERPRISE & SOCIETAL RISKS



Multi- player mitigation & management. Understand in context of your organisations AI Use.



User Risk examples (every transaction)

- Errors & Mistakes, Hallucination — AI can be confidently wrong. HITL
- Model “Behaviour Alignment ” & developers’ values/ interests.
- Automation & ”finished article” bias — don't trust AI over your own judgment
- Data leakage — sensitive data shared with AI tools, often undetected
- Shadow AI — unapproved tools are a leading breach cause. Not approved? Don't use it.
- Security breaches from tools (actions, plug-ins, connections) and apps built by non-technical expertise (vibe coding).
- Prompt injection — hidden in chatbots, documents, sites, memory feature exploitation. Instructions can be circumvented with clever prompting (Gandalf project)
- Agentic AI — systems that access data, take actions and move information externally
- Model drift — vendors update without notice; today's tool ≠ last month's tool for you prompts and tools you build.
- Malicious code in open-source models
- New threats require new controls
- etc.

A Prompting Readiness Check List for Internal Auditors

✓ Safety First

- Privacy & Security (systems and in prompts eg. Prompt injections)
- Follow Organisation AI Policy
- GDPR etc
- Model Training & Retention Policy
- Copyright awareness – in its's training and your use!



✓ Realistic Expectations

- It's a prediction engine – converts text to numbers!
- It's can't make judgements.
- Deterministic vs **Probabilistic**: Understand when to use it, combine it.
- Different models will give different results (alignment training etc) – different “chats” within the same model will give different results.
- It will still make mistakes no matter what you do!



✓ Understand Limitations & Capabilities eg. Some examples

- A base LLM is not a calculator!
 - It predicts numbers, or
 - It writes code for other tools to handle the maths!
- It is not a vast database of knowledge. There is no right or wrong check!
- Their training has cut off dates! That's where the web comes in!



✓ Human – In – The – Loop (HITL)

- You are a key control!
- The critical mind / professional scepticism is essential (GIAS 4.3)
- Don't abdicate your thinking and find ways to exercise your brain!



✓ Love it & Hate it at the same time!

- Amplifier for good and bad outcomes.
- Understand the risks throughout the life cycle.
- AI governance and Assurance is a critical area for Internal Audit.
- 2 (you) Plus 2 (Ai) can be more or less than 4: Uneven Competence



✓ Adopt Fast, Develop Slow

- Study = AI literacy | Use = AI Fluency.
- Start with augmentation.
- Autonomy & agency requires (new) controls and structure (organisationally and technically (eg data). Risks still not fully understood.
- Prompting frameworks = training wheels to get you started, not a strait jacket. An holistic AI Mindset is the real goal!
- Many prompt frameworks exist; This is just one of them.



SESSION 4

The Principles Of Prompting And Prompt Engineering For Internal Auditors

Background of the Framework

- The framework is based on how I work with the models and has been developed through an Internal Audit / GRC lens.
- Many frameworks exist, many overlap, many are subsets of a larger framework – find the one that works for you.
- Prompting is how we (currently) interact with LLM's, you can write it, speak it, copy paste into it, add files, but we need to tell it /show it what we want somehow.
- Because these models can do so much it is up to the user to explore capabilities and limitations ... there is no “instruction manual” in the traditional sense.

Prompting is not a panacea for all ill's

- **Prompting and prompting strategies are only ever a guide, a steer, always open to interpretation, it is never a hardwired command or immutable set of deterministic rules.**
- **It does not circumvent the probabilistic nature of these models output.**
- **Good prompting and other skills can improve the quality of response but never eliminate the chance of “hallucination”, which is in fact a feature of the systems design rather than a bug!**

An auditor's arsenal for improving quality is always evolving ...

Your Critical Mind: GIAS 4.3 Professional Skepticism

Understanding how these models actually work is important!

Understand what they are good at, what they are not good at.

Good Prompting practices ←

Verification built into you work-flows (HITL).

Other suggestions ...?

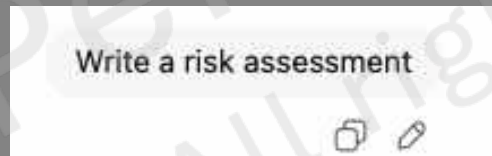
The Basic Prompt

Let's start at the beginning. What happens when you type just four words into an LLM model like ChatGPT?

Start at the Beginning: The Basic Prompt

- Good for that ad hoc exploration, quick question, spontaneous research.
- Making use of the vast general, broad training in the LLM
- You will get back what the model determines is a suitable response based on it's training.

Write a risk assessment



Risk Assessment

1. Purpose

This risk assessment identifies potential hazards associated with the activity/project, evaluates the likelihood and impact of those risks, and outlines control measures to reduce them to an acceptable level.

2. Scope

This assessment applies to all personnel involved in the activity/project, including employees, contractors, visitors, and any other affected parties.

3. Risk Rating Methodology

Risks are evaluated using the following criteria: - **Likelihood:** Rare, Unlikely, Possible, Likely, Almost Certain - **Impact:** Minor, Moderate, Major, Severe - **Risk Level:** Low, Medium, High, Extreme (based on combined likelihood and impact)

4. Identified Risks and Control Measures

Risk ID	Hazard / Risk Description	Who May Be Harmed	Likelihood	Impact	Risk Level	Existing Controls	Additional Controls Required	Responsible Person	Review Date
R1	Example: Slips, trips, and falls	Staff, visitors	Possible	Moderate	Medium	Good housekeeping, signage	Non-slip flooring, regular inspections	Site Manager	DD/MM/YYYY
R2	Example: Equipment failure	Operators	Unlikely	Major	Medium	Preventive maintenance, training	Backup equipment, inspection logs	Operations Lead	DD/MM/YYYY
R3	Example: Fire or electrical hazard	All personnel	Rare	Severe	High	Fire extinguishers, PAT testing	Fire drills, upgraded wiring	H&S Officer	DD/MM/YYYY

5. Emergency Procedures

- Follow site emergency and evacuation procedures
- Report incidents immediately to the responsible person
- Ensure first aid resources are available and accessible

6. Training and Communication

All personnel must receive appropriate training and be informed of identified risks and control measures prior to commencing work.

7. Monitoring and Review

This risk assessment will be reviewed: - After any incident or near miss - When significant changes occur - At least annually

8. Approval

Name	Role	Signature	Date

- It's a risk assessment!
- It's an activity / project (I did not specify)
- It's generic!
- Its vague!
- But it's not not what I asked for!

Getting a better response

If the response is not what was expected, or too vague, or too detailed, or just not what you wanted, how do you guide the model to give something better?

The Impact of the Prompt

The Basic Prompt:

- A simple request in 4 words

Write a risk assessment

The screenshot shows a risk assessment document with several sections. Annotations on the right side of the document point to specific parts:

- It's a risk assessment!
- It's an activity / project (I did not specify)
- It's generic!
- Its vague!
- But it's not not what I asked for!

The document includes sections for: 1. Purpose, 2. Scope, 3. Risk Rating Methodology, 4. Identified Risks and Control Measures (with a table), 5. Emergency Procedures, 6. Training and Communication, 7. Monitoring and Review, and 8. Approval.

The Engineered Prompt

- Structured & c.500 words

Risk Category	Risk Description	Potential Causes	Initial Risk Rating	Mitigation Suggestions	Reasoning
Supply Chain	Failure or disruption of critical component supply	Geopolitical conflict, sanctions, single-source suppliers, logistics failures	High	Dual sourcing, supplier risk scoring, regional buffers, supplier audits	Global footprint, heavy reliance on specialised components, exposure to China/Vietnam and geopolitically sensitive regions
Supply Chain	Ethical, ESG, or compliance failure within supplier base	Limited visibility beyond Tier 1, weak ESG controls in emerging markets	High	Supplier code of conduct, ESG audits, contractual rights to inspect	Large supplier base (3,000), regulatory and reputational exposure
Production	Manufacturing quality failures leading to product recalls	Design flaws, process variation, inadequate QA, supplier defects	High	Enhanced quality gates, digital QA systems, design-for-safety reviews	Heavy lifting equipment carries high safety and liability exposure
Product Liability	Catastrophic failure of cranes or lifting equipment	Design defects, improper installation, misuse, poor maintenance	High	Robust design validation, field data monitoring, liability insurance	Core risk for any heavy equipment manufacturer
Workforce Safety	Serious injury or fatality in manufacturing or field service	Hazardous environments, inconsistent safety culture, contractor risks	High	Global H&S framework, ISO 45001 alignment, contractor safety controls	High-risk physical operations across 70 countries
Regulatory Compliance	Non-compliance with local manufacturing, safety, or trade regulations	Complex multi-jurisdictional requirements, weak local oversight	High	Central compliance function, regulatory mapping, training	Operates in 70 countries with varying regulatory maturity
Financial	Liquidity or cash flow stress	Revenue volatility, long receivables cycles, project delays	High	Cash forecasting, milestone billing, credit controls	Board-identified concern; capital-intensive business
Financial	Revenue recognition errors	Complex contracts, aftermarket services, inconsistent application of accounting standards	Medium-High	Contract review controls, accounting policy standardisation	Significant judgement involved in long-term and service contracts
Fraud & Corruption	Bribery, kickbacks, or facilitation payments	Third-party agents, high-risk countries, sales incentives	High	Anti-bribery program, third-party due diligence, whistleblowing	Use of agents in 30 countries, enforcement trend risk
Third Parties	Failure or misconduct by third-party sales or service partners	Weak oversight, misaligned incentives, capability gaps	High	Partner governance model, audits, performance KPIs	Direct impact on brand, safety, and compliance
Cybersecurity	Cyberattack disrupting operations or IP theft	Legacy OT systems, ransomware, phishing	High	NIST CSF alignment, OT security segmentation, incident response plans	Increasing attacks on manufacturing and OT environments
Technology	Inappropriate or uncontrolled use of AI and digital tools	Lack of governance, poor data quality, regulatory uncertainty	Medium	AI governance framework, use-case approval, data controls	Emerging risk highlighted by Board; regulatory scrutiny increasing

The improved response

HG Movement – 1st Pass Enterprise-Level Risk Assessment

Purpose

This document provides a *first-pass* Enterprise Risk Assessment for HG Movement, intended to support Board and Executive discussion and prioritisation. It is aligned conceptually with ISO 31000 and COSO ERM (2017) principles and reflects HG Movement’s global manufacturing, sales, and aftermarket service footprint.

This assessment is **not exhaustive** and is designed to be refined through workshops, risk quantification, and alignment to HG Movement’s risk appetite.

Methodology & Standards Referenced

The following frameworks and standards were considered conceptually in structuring this assessment:

- **ISO 31000:2018 – Risk Management Guidelines**
<https://www.iso.org/standard/65694.html>
- **COSO Enterprise Risk Management – Integrating with Strategy and Performance (2017)**
<https://www.coso.org/Shared%20Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf>
- **OECD Guidelines for Multinational Enterprises** (for third-party, corruption, and supply chain considerations)
<https://www.oecd.org/investment/mne/>
- **NIST Cybersecurity Framework (CSF)** (high-level reference)
<https://www.nist.gov/cyberframework>

Important disclosure on sources used:

This assessment did **NOT** use full proprietary source documentation of ISO, COSO, or NIST standards. It is based on **publicly available executive summaries documents, and generally accepted industry interpretations** of these frameworks, including third-party guides and practitioner experience.

Risk Rating Approach (Initial / Inherent)

- **High** – Could materially impact safety, regulatory standing, liquidity
- **Medium** – Could disrupt operations or financial performance if not
- **Low** – Manageable with routine controls

Ratings reflect *inherent risk* prior to additional mitigation refinement.

Enterprise Risk Register – 1st Pass					
Risk Category	Risk Description	Potential Causes	Initial Risk Rating	Mitigation Suggestions	Reasoning
Supply Chain	Failure or disruption of critical component supply	Geopolitical conflict, sanctions, single-source suppliers, logistics failures	High	Dual sourcing, supplier risk scoring, regional buffers, supplier audits	Global footprint, heavy reliance on specialised components, exposure to China/Vietnam and geopolitically sensitive regions
Supply Chain	Ethical, ESG, or compliance failure within supplier base	Limited visibility beyond Tier 1, weak ESG controls in emerging markets	High	Supplier code of conduct, ESG audits, contractual rights to inspect	Large supplier base (3,000), regulatory and reputational exposure
Production	Manufacturing quality failures leading to product recalls	Design flaws, process variation, inadequate QA, supplier defects	High	Enhanced quality gates, digital QA systems, design-for-safety reviews	Heavy lifting equipment carries high safety and liability exposure
Product Liability	Catastrophic failure of cranes or lifting equipment	Design defects, improper installation, misuse, poor maintenance	High	Robust design validation, field data monitoring, liability insurance	Core risk for any heavy equipment manufacturer
Workforce Safety	Serious injury or fatality in manufacturing or field service	Hazardous environments, inconsistent safety culture, contractor risks	High	Global H&S framework, ISO 45001 alignment, contractor safety controls	High-risk physical operations across 70 countries
Regulatory Compliance	Non-compliance with local manufacturing, safety, or trade regulations	Complex multi-jurisdictional requirements, weak local oversight	High	Central compliance function, regulatory mapping, training	Operates in 70 countries with varying regulatory maturity
Financial	Liquidity or cash flow stress	Revenue volatility, long receivables cycles, project delays	High	Cash forecasting, milestone billing, credit controls	Board-identified concern; capital-intensive business
Financial	Revenue recognition errors	Complex contracts, aftermarket services, inconsistent application of accounting standards	Medium-High	Contract review controls, accounting policy standardisation	Significant judgement involved in long-term and service contracts
Fraud & Corruption	Bribery, kickbacks, or facilitation payments	Third-party agents, high-risk countries, sales incentives	High	Anti-bribery program, third-party due diligence, whistleblowing	Use of agents in 30 countries, enforcement trend risk
Third Parties	Failure or misconduct by third-party sales or service partners	Weak oversight, misaligned incentives, capability gaps	High	Partner governance model, audits, performance KPIs	Direct impact on brand, safety, and compliance
Cybersecurity	Cyberattack disrupting operations or IP theft	Legacy OT systems, ransomware, phishing	High	NIST CSF alignment, OT security segmentation, incident response plans	Increasing attacks on manufacturing and OT environments
Technology	Inappropriate or uncontrolled use of AI and digital tools	Lack of governance, poor data quality, regulatory	Medium	AI governance framework, use-case approval, data	Emerging risk highlighted by Board; regulatory scrutiny increasing

Appendix A – Risks Considered but Not Included

Risk	Reason for Exclusion
Currency exchange volatility	Considered a normal financial management risk at this stage; expected to be handled via treasury policies
Pension funding risk	No specific information provided on defined benefit exposure
Tax structuring risk	Requires deeper legal and jurisdictional analysis beyond first pass
Environmental pollution events	Partially embedded within regulatory and reputational risks; can be separated in later iterations
IT system obsolescence	Considered a sub-component of cybersecurity and technology risks

Next Steps (Recommended)

1. Validate risk list with Executive and Board
2. Define risk appetite statements
3. Perform residual risk assessment
4. Assign risk ownership
5. Integrate into COSO ERM-aligned risk reporting

Prepared as an initial enterprise risk perspective for HG Movement. To be refined through further analysis and workshops.

Reasoning
Core competitive advantage tied to design

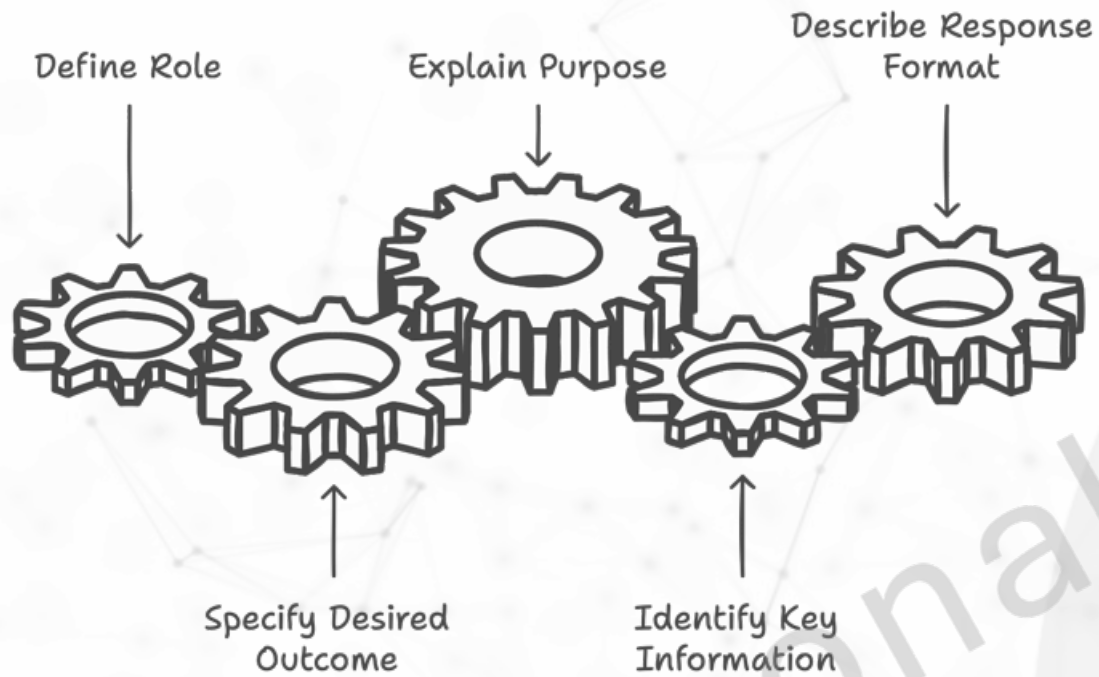
Explicit Board concern; exposure in multiple high-risk regions

Global brand with safety-critical products

Six manufacturing sites represent concentration risk

Sales and service presence in EU and globally

Competitive and technology-driven industry



You can, to a certain extent, think of Good Prompting as Good Communication & Supervision!

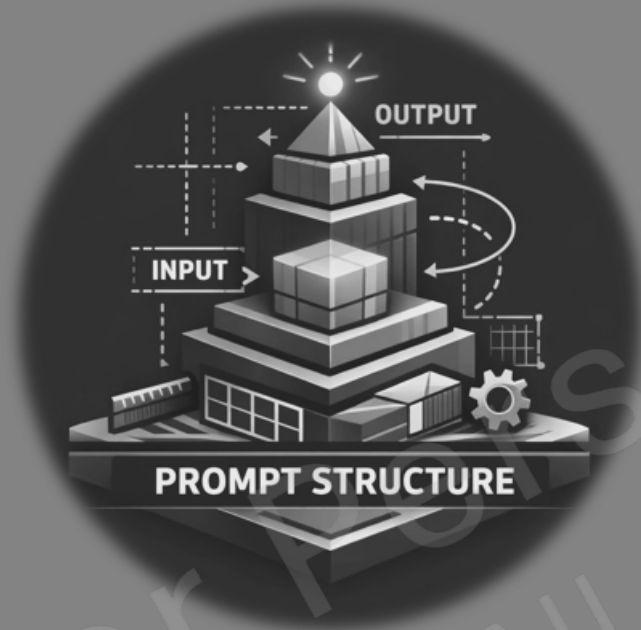
This is Prompt Engineering

Building a better prompt to give a better response – tell it what its role is, tell it what you want, why you want it, what is important to know, and how you want the response to look and “feel”!

We will not go through the following slide by slide – it is there as a reference for you to come back to.

How I write an Engineered Prompt

STRUCTURE



What you say!

The components of a good prompt.



STYLE

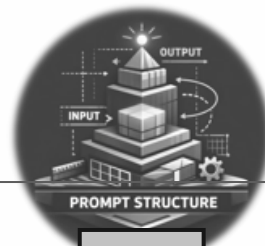


How you say it!

The effectiveness of a good prompt.

PROMPT

STRUCTURE



R O C K V O P

<u>R</u> OLE	<u>O</u> BJECTIVE	<u>C</u> ONTEXT	<u>K</u> NOWLEDGE	<u>V</u> OICE	<u>O</u> UTPUT	<u>P</u> RINCIPLES
<p>Give it a ROLE:</p> <p>Assign a specific role or identity to the model eg. "Act as a expert Risk Management Consultant", "Act as a qualified Internal Auditor specialising in I.T"</p>	<p>Give it an OBJECTIVE / TASK to accomplish:</p> <p>eg. "Create a risk assessment for" or "Coach me through the proces of creating a risk assessment for"</p>	<p>Give it a CONTEXT :</p> <p>Why is it needed; Who is it for, Important specifics, background, docs to be analysed, examples, refs..</p>	<p>Give it / point it to specific KNOWLEDGE to use in preparing its response:</p> <p>Specify method, standard, framework to apply if appropriate. If specialized or bespoke detail it in the prompt or add a document</p>	<p>Tell it what VOICE or TONE to respond in:</p> <p>eg. "Use a professional and supportive tone, with a focus on providing practical advice and actionable insights."</p>	<p>Tell it what OUTPUT you want and in what FORMAT:</p> <p>eg. "The response should be structured in bullet points with clear headings for each section. The entire response should be concise, no longer than 500 words".</p>	<p>Tell it what PRINCIPLES* (rules/behaviours) to follow :</p> <p>eg. "Always acknowledge when information is uncertain, never present opinions as facts, and when discussing controversial topics, always present multiple viewpoints."</p>
<p>It frames or grounds the model's perspective and expertise, helping it provide more relevant responses.</p>	<p>It provides clear instructions on what needs to be done, ensuring the response is goal-oriented.</p>	<p>It helps model to understand background & nuances, makes the response more accurate and insightful. Describing the intended use adds context also.</p>	<p>Often added into GPTS, Gems or added in skills Characterised by something that is constant (just update when revised or new version released)</p>	<p>Setting the tone ensures the response is appropriate for its audience and effectively conveys the intended message.</p>	<p>Defining the output format enhances the usability of the response and ensures the structure matches your needs.</p>	<p>Guides the model on the behaviours and preferred methods to use and sequence in interaction. Eg. workflow, Critical thinking, alternatives etc.</p>

**Principles can benefit from being placed early in a longer prompt, and even repeated at the end in very long long prompts*

PROMPT

STYLE



C

R

I

M

P

CLEAR

Clearly written instructions that are logical and specific.
Break down long instructions for complex tasks.
“Chunking” or Prompt Chaining

It helps the model understand complex tasks more effectively, reducing the chance of misinterpretation.

REFINE

Iterate & Refine
Clarify ambiguities, tailor outputs to your needs, improve accuracy.
Makes your prompts better going forward

Can be seen as a form of 'co-creation,' where both the user and the model collaborate to refine and improve the response iteratively, making it a collaborative effort to achieve the best possible outcome.

ILLUSTRATE

Provide examples to show what you mean, demonstrating desired format, style, or approach. Input / Output examples

Sometimes call Few Shot, One Shot prompting – each “Shot” is one example or illustration.
Zero-Shot (No Example) - You describe what you want without providing an example.

MARK-UP

“Markdown / XML/JSON”: Format the prompt using gaps, spaces, symbols, delimiters. Easier for the model to process.

It makes the structure of your request clearer, allowing for easier parsing of multiple tasks or sections. Use mostly in Scripts, Custom Instructions, Agent Instructions, Very large Prompts.

PRECISE

Precise choice and use of words and action verbs. Eg. Create, Analyse, Review, Summarise, Perform etc.

It narrows down the scope, ensuring the response targets exactly what you intend.

PROMPT



STRUCTURE

R **O** **C** **K** **V** **O** **P**

ROLE

Give it a **ROLE**:

Assign a specific role or identity to the model
eg. "Act as a expert Risk Management Consultant" , , .
"Act as a qualified Internal Auditor specialising in I.T"

It frames or grounds the model's perspective and expertise, helping it provide more relevant responses.

EXAMPLES

- "As an experienced internal auditor, conduct a risk assessment of the company focusing on financial reporting risks."
- "As a Chief Risk Officer, evaluate the effectiveness of the company's current risk mitigation strategies."
- "As a cybersecurity consultant, identify key vulnerabilities in the company's IT infrastructure."
- "As a business continuity expert, assess the risks to the company's supply chain during a major disruption."

IMPACT ON RESPONSE

What risks are there?



Act as an internal auditor, what risks are there?



What risks are there?

What risks are there?

I need a bit more context to answer that accurately. **Risks of what, specifically?**

For example, are you asking about:

- A business decision or investment
- A medical treatment or health choice
- A technology or AI tool
- A legal agreement or contract
- A travel plan or activity
- A project at work or school

Tell me the situation (even briefly), and I'll outline the key risks, how serious they are, and how they can be mitigated.



Act as an internal auditor, what risks are there?

As an internal auditor, I'd first clarify **the scope**, because "what risks are there?" depends heavily on **what area, process, or objective** we are reviewing.

That said, auditors usually think in **risk categories**. Below is a practical, high-level risk universe that applies to most organizations, which we then tailor to the specific area under review.

1. Strategic Risks

Risks that affect the organization's ability to achieve its objectives.

- Poor or unclear strategy
- Misalignment between strategy and operations
- Inadequate response to market, regulatory, or technological change
- Overreliance on key customers, suppliers, or individuals
- Mergers/acquisitions not delivering expected value

2. Operational Risks

Risks arising from day-to-day activities and processes.

- Inefficient or undocumented processes
- Inadequate segregation of duties
- Human error or lack of training
- Business continuity and disaster recovery weaknesses
- Health & safety incidents
- Supply chain disruptions

3. Financial Risks

Risks impacting financial accuracy and stability.

- Errors or fraud in financial reporting
- Weak internal controls over cash, revenue, or expenses
- Inaccurate budgeting or forecasting
- Liquidity or cash-flow issues
- Unauthorized transactions
- Asset misappropriation

4. Compliance & Legal Risks

Risks of violating laws, regulations, or internal policies.

- Non-compliance with laws and regulations
- Failure to follow internal policies or procedures
- Inadequate monitoring of regulatory changes
- Contractual non-compliance
- Data privacy or employment law breaches

5. IT & Cyber Risks

Risks related to systems, data, and technology.

- Cybersecurity threats (hacking, ransomware)
- Inadequate access controls
- Data integrity or data loss
- System outages or poor change management
- Lack of backup and recovery testing
- Overdependence on third-party IT providers

6. Fraud Risks

Intentional acts to obtain an unfair or illegal advantage.

- Management override of controls
- Procurement fraud or conflicts of interest
- Payroll or expense fraud
- Revenue manipulation
- Weak whistleblowing mechanisms

7. Reputational Risks

Risks that could damage trust and credibility.

- Poor customer service
- Ethical breaches
- Publicized compliance failures
- Data breaches
- Poor handling of complaints or incidents

8. Governance Risks

Risks related to oversight and decision-making.

- Weak board or management oversight
- Lack of clear accountability
- Poor risk management framework
- Inadequate internal audit independence
- Tone at the top not supporting ethical behavior

How an Internal Auditor Uses This

An internal auditor would:

1. Identify which of these risks apply to the **specific area under review**
2. Assess **likelihood and impact**
3. Evaluate whether **controls exist and are effective**
4. Report **gaps, root causes, and recommendations**

Act as an internal auditor, what risks are there?

- First states what an IA should really do, then offers high level generic answer!
- BUT, grounded in the world of IA!

PROMPT



STRUCTURE

R O C K V O P

OBJECTIVE

Give it an **OBJECTIVE / TASK** to accomplish:
eg. "Create a risk assessment for" or "Coach me through the process of creating a risk assessment for"

It provides clear instructions on what needs to be done, ensuring the response is goal-oriented.

EXAMPLES

- "Perform a risk assessment of the company's supply chain processes."
- "Identify and list the top five strategic risks facing the company."
- "Analyze the effectiveness of the company's internal controls for financial reporting."
- "Evaluate the potential impact of regulatory changes on the company's compliance framework."

IMPACT ON RESPONSE

Act as an internal auditor, what risks are there?



Act as an internal auditor, perform a risk assessment of the 10 most critical risks.



Below is a generic enterprise-wide internal audit risk assessment commonly applicable to medium-large organizations across specific sector, geography, or maturity level if needed.

Enterprise Risk Assessment – Top 10 Critical Risks

Perspective: Internal Audit

Objective: Identify, prioritize, and assess risks that could materially impact operations, financial reporting, compliance, and reputation.

Risk Rating Methodology (assumed)

- **Impact:** Low / Medium / High / Severe
- **Likelihood:** Low / Medium / High
- **Inherent Risk:** Before controls
- **Residual Risk:** After existing controls

1. Cybersecurity & Data Breach Risk

- **Description:** Unauthorized access, ransomware, or data loss of proprietary data.
- **Impact:** Severe (financial loss, regulatory penalties, reputation damage)
- **Likelihood:** High
- **Inherent Risk:** Very High
- **Key Controls:**
 - Security monitoring (SIEM, SOC)
 - Access controls & MFA
 - Incident response plan
- **Residual Risk:** High
- **Audit Focus:** Cyber maturity, third-party access, incident response

2. Regulatory & Legal Non-Compliance

- **Description:** Failure to comply with laws, regulations, or industry standards.
- **Impact:** High
- **Likelihood:** Medium-High
- **Inherent Risk:** High
- **Key Controls:**
 - Compliance framework
 - Legal review processes
 - Training & compliance monitoring
- **Residual Risk:** Medium-High
- **Audit Focus:** Regulatory change management, compliance monitoring

3. Financial Reporting & Fraud Risk

- **Description:** Material misstatement due to error or fraud in financial reporting.
- **Impact:** High
- **Likelihood:** Medium
- **Inherent Risk:** High
- **Key Controls:**
 - Segregation of duties
 - Reconciliations
 - Management review controls
- **Residual Risk:** Medium
- **Audit Focus:** Journal entries, management override, revenue recognition

4. Third-Party & Vendor Risk

- **Description:** Operational, financial, or compliance failure by critical suppliers or vendors.
- **Impact:** High
- **Likelihood:** Medium-High
- **Inherent Risk:** High
- **Key Controls:**
 - Vendor due diligence
 - SLAs and monitoring
 - Business continuity requirements
- **Residual Risk:** Medium-High
- **Audit Focus:** Vendor risk assessments, subcontracting oversight

5. Business Continuity & Disaster Recovery Risk

- **Description:** Inability to continue operations due to major disruption (e.g., natural disaster, geopolitical event).
- **Impact:** Severe
- **Likelihood:** Medium
- **Inherent Risk:** High
- **Key Controls:**
 - BCP/DR plans
 - Backup systems
 - Regular testing
- **Residual Risk:** Medium-High
- **Audit Focus:** Plan testing, recovery time objectives (RTOs)

6. Strategic & Market Risk

- **Description:** Poor strategic decisions or failure to adapt to market, technology, or competitive changes.
- **Impact:** High
- **Likelihood:** Medium
- **Inherent Risk:** High
- **Key Controls:**
 - Strategic planning process
 - Board oversight
 - Market intelligence
- **Residual Risk:** Medium
- **Audit Focus:** Governance, decision-making quality, KPIs

7. Operational Process Failure

- **Description:** Inefficient or ineffective core processes leading to errors, delays, or cost overruns.
- **Impact:** Medium-High
- **Likelihood:** High
- **Inherent Risk:** High
- **Key Controls:**
 - Standard operating procedures
 - Performance metrics
 - Quality assurance
- **Residual Risk:** Medium
- **Audit Focus:** End-to-end process reviews

8. Human Capital & Talent Risk

- **Description:** Loss of key personnel, skills gaps, or poor succession planning.
- **Impact:** Medium-High
- **Likelihood:** Medium-High
- **Inherent Risk:** Medium-High
- **Key Controls:**
 - Succession planning
 - Training programs
 - Retention strategies
- **Residual Risk:** Medium
- **Audit Focus:** Critical role dependency, workforce planning

9. Ethics & Conduct Risk

- **Description:** Unethical behavior, conflicts of interest, harassment, or corruption.
- **Impact:** High
- **Likelihood:** Medium
- **Inherent Risk:** High
- **Key Controls:**
 - Code of conduct
 - Whistleblower mechanisms
 - Ethics training
- **Residual Risk:** Medium
- **Audit Focus:** Culture assessment, hotline effectiveness

10. Data Integrity & Management Information Risk

- **Description:** Inaccurate, incomplete, or untimely data used for decision-making.
- **Impact:** Medium-High
- **Likelihood:** Medium
- **Inherent Risk:** Medium-High
- **Key Controls:**
 - Data governance
 - Validation controls
 - Reporting reconciliations
- **Residual Risk:** Medium
- **Audit Focus:** Data lineage, critical reports, system interfaces

Overall Internal Audit Observations

- **Top Residual Risks:** Cybersecurity, third-party risk, regulatory compliance
- **Common Control Gaps:** Monitoring effectiveness, third-party oversight, incident preparedness
- **Audit Priority Areas:** IT & cyber audits, compliance reviews, vendor management, financial controls

 **perform**
/pə'fɔ:m/

verb

1. carry out, accomplish, or fulfil (an action, task, or function).
"I have my duties to perform"

+

“Risk Assessment”

+

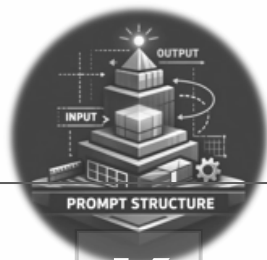
“Internal Auditor”

=

- *More specific risk identification*
- *Risk Impact & Likelihood*
- *Description of Key Controls*
- *Audit Focus*

... so much more than when you asked
“what are the risks”!

PROMPT



STRUCTURE

R O C K V O P

CONTEXT IS EVERYTHING!
*Put the unique knowledge needed in
the prompt (context window)*

PROMPT



STRUCTURE

R O C K V O P

CONTEXT

Give it a **CONTEXT** :
Why is it needed; Who is it for,
Important specifics,
background, docs to be
analysed, examples, refs..

It helps model to understand
background & nuances, makes the
response more accurate and
insightful. Describing the intended
use adds context also.

EXAMPLES

- *"Conduct a risk assessment of the company, focusing on operational risks related to logistics. The assessment is for the upcoming board meeting, and it should include both past incidents and mitigation strategies." **Past incidents and mitigations are as follows**"*
- *"Assess the compliance risks of the company's new product launch, considering recent regulatory changes in the industry. The report is for the compliance department."*
- **Facts, Background, Examples – "Few Shots (see illustrate also)**

IMPACT ON RESPONSE

Act as an internal auditor, perform a risk assessment of the 10 most critical risks.

Act as an internal auditor, perform a risk assessment of the top 10 most critical risks in the operations of a medium sized vehicle manufacturing company. The company has an assembly factories in the UK and Poland, and a components fabrication factory in China. The company sources other key components and parts from suppliers across the world.

Detailed Risk Assessment

1. Global Supply Chain Disruption

Risk Description

Disruption to the supply of critical components due to supplier failure, logistics delays, or geopolitical tensions.

Key Risk Drivers

- Heavy reliance on overseas suppliers
- Long lead times and just-in-time inventory
- Limited alternative or dual sourcing options

Potential Impact

- Production stoppages in UK and EU
- Missed customer deliveries
- Revenue loss and reputational damage

Expected Key Controls / Mitigation

- Dual/multi-sourcing strategies
- Supplier risk scoring and monitoring
- Safety stock policies for high-risk components
- Business continuity plans for critical suppliers

2. Trade Restrictions, Tariffs & Sanctions

Risk Description

Changes in trade policy affecting import/export duties, sanctions, export controls, or trade agreements.

Key Risk Drivers

- China-based fabrication facilities
- Brexit-related UK-EU customs changes
- Heightened geopolitical tensions

Potential Impact

- Increased cost of goods sold
- Customs delays affecting production
- Forced supplier or footprint changes

Expected Key Controls

- Trade compliance monitoring
- Scenario planning for tariff changes
- Use of bonded warehouses / customs brokers
- Legal review of sanctions exposure

3. Manufacturing Downtime & Capacity Constraints

Risk Description

Unplanned downtime due to equipment failure, maintenance issues, or production bottlenecks.

Key Risk Drivers

- Capital-intensive machinery
- Aging production equipment
- High utilization rates

Potential Impact

- Lost production volume
- Overtime and expedited shipping costs
- Reduced operating efficiency

Expected Key Controls

- Preventive and predictive maintenance
- Overall Equipment Effectiveness (OEE) monitoring
- Spare parts strategy for critical machinery
- Capacity contingency planning

4. Product Quality & Recall Risk

Risk Description

Defective components or assembly errors leading to customer complaints, recalls, or safety incidents.

Key Risk Drivers

- Complex global supply chain
- Inconsistent supplier quality standards
- Process deviations at plants

Potential Impact

- Costly recalls and warranty expenses
- Regulatory penalties
- Brand damage and customer trust erosion

Expected Key Controls

- Robust Quality Management System (IATF 16949)
- Supplier audits and PPAP processes
- End-of-line and in-process testing
- Root cause analysis and corrective actions

5. Regulatory & Homologation Non-Compliance

Risk Description

Failure to comply with vehicle safety, emissions, environmental, or other regulatory requirements across different jurisdictions.

Key Risk Drivers

- Differing UK, EU, and Chinese regulations
- Frequent regulatory changes (e.g., emissions standards)
- Inadequate regulatory monitoring

Potential Impact

- Sales bans or delayed vehicle launches
- Fines and legal exposure
- Re-engineering costs

Expected Key Controls

- Centralized regulatory compliance function
- Change management for regulatory updates
- Independent compliance testing and certification
- Internal compliance audits

6. Cost Volatility & Margin Erosion

Risk Description

Uncontrolled increases in raw materials, energy, labor, and logistics costs.

Key Risk Drivers

- Steel, aluminum, battery material price swings
- Energy price volatility (especially in Europe)
- FX exposure (GBP, EUR, CNY, USD)

Potential Impact

- Reduced margins
- Pricing pressure in competitive markets
- Budget and forecast inaccuracies

Expected Key Controls

- Commodity hedging strategies
- Long-term supplier contracts
- FX risk management policies
- Cost transparency and variance analysis

7. Environmental, Social & Labor Compliance (ESG)

Risk Description

Non-compliance with environmental standards or labor practices, leading to fines, reputational damage, or operational disruptions.

Key Risk Drivers

- Diverse regulatory environments
- Supplier ESG maturity gaps
- Increased stakeholder scrutiny

Potential Impact

- Fines and shutdowns
- Loss of OEM or fleet customers
- Reputational damage

Expected Key Controls

- ESG policy and supplier code of conduct
- Environmental monitoring and reporting
- Supplier audits (labor, health & safety)
- Sustainability KPIs and disclosures

8. Cybersecurity & OT System Vulnerability

Risk Description

Cyberattacks targeting IT systems, industrial control systems (ICS), or OT systems.

Key Risk Drivers

- Increasing digitization of manufacturing
- Remote access to OT systems
- Third-party IT dependencies

Potential Impact

- Production stoppages
- Theft of IP or designs
- Ransom payments and recovery costs

Expected Key Controls

- Network segmentation (IT vs OT)
- Regular penetration testing
- Incident response and recovery plans
- Cyber awareness training

9. Skills Shortages & Labor Relations

Risk Description

Inability to attract or retain skilled engineers, technicians, or production staff; labor disputes.

Key Risk Drivers

- Tight labor markets in UK/EU
- Aging workforce
- Unionized environments

Potential Impact

- Reduced productivity
- Increased defect rates
- Disruption from strikes or absenteeism

Expected Key Controls

- Workforce planning and succession management
- Training and upskilling programs
- Employee engagement initiatives
- Contingency staffing plans

10. Single-Point-of-Failure Facilities

Risk Description

Over-reliance on a single fabrication plant in China or unique equipment without alternatives.

- Risks grounded in Manufacturing
- International trade
- Less generic
- More relevant

- Mapping of single points of failure
- Strategic footprint diversification analysis
- Insurance coverage review

Internal Audit Observations (Overall)

- Supply chain and geopolitical risks are the most critical due to global complexity.
- Quality, compliance, and cyber risks pose significant downside and reputational exposure.
- Risk maturity often varies significantly between European operations and China-based manufacturing.
- Strong governance, data visibility, and supplier oversight are key risk differentiators.

PROMPT



STYLE

C

R

I

M

P

PRECISE

Precise choice and use of words and action verbs. Eg. Create, Analyse, Review, Summarise, Perform etc.

It narrows down the scope, ensuring the response targets exactly what you intend.

EXAMPLES

- *"Analyse and summarise the top operational risks affecting the company's supply chain, including potential mitigation strategies."*
- *"Create a detailed evaluation of the financial risks involved in the company's expansion into new markets, focusing on currency fluctuations."*
- *"Review and rank the top five strategic risks the company faces and suggest mitigation approaches for each."*
- *"Summarise the compliance risks related to data privacy laws, specifying areas where the company is at the highest risk of non-compliance."*

IMPACT ON RESPONSE

"PERFORM" a risk assessment

Vs

Act as an internal auditor, SUMMARISE the top 10 most critical risks in the operations of a medium sized vehicle manufacturing company. The company has an assembly factories in the UK and Poland, and a components fabrication factory in China. The company sources other key components and parts from suppliers across the world.

Below is a concise internal-audit-style summary of the **Top 10 Most Critical Operational Risks** for a medium-sized vehicle manufacturing company with assembly plants in the UK and Poland, a components factory in China, and a global supplier base.

Risks are ranked by **potential impact and likelihood**, considering operational, regulatory, financial, and reputational exposure.

Top 10 Critical Operational Risks

1. Supply Chain Disruption & Dependency Risk

Risk: Over-reliance on single or geographically concentrated suppliers for critical components (e.g. semiconductors, powertrain parts).

Impact: Production stoppages, delayed deliveries, revenue loss.

Drivers: Global logistics volatility, geopolitical tensions, supplier financial instability.

2. Geopolitical & Trade Compliance Risk

Risk: Tariffs, sanctions, export controls, or trade restrictions affecting China-EU-UK flows.

Impact: Increased costs, delayed shipments, non-compliance penalties.

Drivers: US-China trade tensions, EU trade policy changes, post-Brexit customs regimes.

3. Quality & Product Safety Risk

Risk: Inconsistent quality standards across manufacturing locations and suppliers.

Impact: Vehicle recalls, warranty costs, regulatory fines, brand damage.

Drivers: Supplier quality lapses, inadequate inspections, process deviations.

4. Regulatory & Environmental Compliance Risk

Risk: Failure to comply with varying environmental, safety, and vehicle regulations across jurisdictions.

Impact: Fines, production shutdowns, loss of operating licences.

Drivers: EU emissions rules, UK HSE requirements, China environmental laws.

5. Operational Continuity & Business Interruption Risk

Risk: Disruption from factory shutdowns, pandemics, natural disasters, or energy shortages.

Impact: Prolonged production downtime and unmet customer demand.

Drivers: Energy price volatility in Europe, climate-related events, geopolitical instability.

6. Labour & Workforce Risk

Risk: Skilled labour shortages, industrial action, or high staff turnover.

Impact: Reduced productivity, increased costs, delayed production schedules.

Drivers: Brexit-related labour constraints, EU labour laws, wage inflation.

7. Cybersecurity & Intellectual Property Risk

Risk: Cyberattacks targeting manufacturing systems or theft of IP through suppliers or overseas operations.

Impact: Production disruption, IP loss, regulatory exposure, reputational damage.

Drivers: Increased digitalisation, weak supplier cyber controls, cross-border data sharing.

8. Financial & Cost Volatility Risk

Risk: Exposure to currency fluctuations, raw material price volatility, and inflation.

Impact: Margin erosion and inaccurate cost forecasting.

Drivers: GBP/EUR/CNY exchange rate movements, commodity price swings.

9. Supplier ESG & Ethical Sourcing Risk

Risk: Suppliers failing to meet environmental, labour, or ethical standards.

Impact: Regulatory sanctions, customer backlash, reputational damage.

Drivers: Limited supplier oversight, evolving ESG expectations, regulatory scrutiny.

10. Production Planning & Inventory Management Risk

Risk: Poor demand forecasting or inventory mismanagement.

Impact: Excess working capital, obsolescence, customer dissatisfaction.

Drivers: Market volatility, inaccurate demand signals.

Key Internal Audit Focus Areas

- Supply chain resilience and dependency
- Supplier risk assessment and ongoing monitoring
- Cross-site quality and compliance standardisation
- Trade compliance and customs controls
- Cybersecurity maturity across operations and suppliers

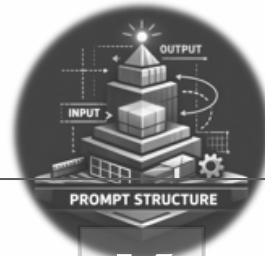
If you wish, I can also:

- Map these risks to **COSO ERM**
- Provide a **risk heat map**
- Identify **key controls and audit tests**
- Tailor the risks to **EV manufacturing or ICE vehicles**

Just let me know.

- *Far briefer, no reference to controls*
- *Style and content seems to assume existing knowledge*

PROMPT



STRUCTURE



VOICE

Tell it what VOICE or TONE to respond in:


eg. "Use a professional and supportive tone, with a focus on providing practical advice and actionable insights."

Setting the tone ensures the response is appropriate for its audience and effectively conveys the intended message.

EXAMPLES

- *"Provide a risk assessment of the company in a formal and authoritative tone, suitable for presentation to senior management."*
- *"Summarize the company's top operational risks in a conversational tone for an internal newsletter."*
- *"Draft a compliance risk report in a concise, professional tone that can be shared with external auditors."*
- *"Explain the potential financial risks in a friendly, easy-to-understand tone for non-financial stakeholders."*

IMPACT ON RESPONSE

Take the previous example and re-iterate: 

This is a very good summary. Please re-write a summary version for use in the monthly Manufacturing Operations Team Newsletter to employees. The purpose of the article to inform the team members of the types of risks faced and the types of actions needed to address them. Keep the tone conversational and constructive.



Understanding the Key Risks in Our Manufacturing Operations

As a global vehicle manufacturer with operations in the UK, Poland, China, and suppliers around the world, our success depends on **many moving parts working smoothly together**. Like any complex operation, we face a range of risks — understanding them helps us **spot issues early and take the right actions**.

Below is a simple overview of the **main types of operational risks we manage every day**, and how everyone plays a role in reducing them.

1. Keeping Our Supply Chain Moving

Delays or shortages of parts can slow production very quickly. We work to reduce this risk by planning ahead, using multiple suppliers where possible, and staying in close contact with our partners.

How you help: Flag supply concerns early and follow escalation processes.

2. Navigating Global Trade & Regulations

Different countries mean different rules — from customs and tariffs to import/export controls. Staying compliant avoids delays and unexpected costs.

How you help: Follow procedures carefully and raise questions when something doesn't look right.

3. Protecting Quality & Product Safety

Quality issues don't just affect one vehicle — they affect our reputation. Consistent standards across all sites and suppliers are critical.

How you help: Follow quality checks, report defects, and support continuous improvement.

4. Meeting Environmental & Safety Requirements

We operate under strict environmental and safety regulations in every country. Getting this right protects our people, our communities, and our licence to operate.

How you help: Work safely, follow environmental controls, and report incidents or near misses.

5. Avoiding Production Disruptions

Unexpected events — from energy shortages to extreme weather — can impact production. Planning and flexibility help us respond quickly.

How you help: Stick to contingency plans and communicate issues early.

6. Supporting Our Workforce

Skilled people keep our factories running. Labour shortages, training gaps, or industrial action can affect output and morale.

How you help: Share knowledge, support training, and raise workforce concerns constructively.

7. Staying Cyber-Safe

Modern manufacturing relies on digital systems. Cyber risks can disrupt operations or expose sensitive information.

How you help: Follow IT security rules and stay alert to suspicious activity.

8. Managing Costs & Financial Pressures

Currency movements, energy prices, and raw material costs can change quickly. Managing waste and efficiency helps protect margins.

How you help: Use materials responsibly and support cost-saving initiatives.

9. Working with Responsible Suppliers

Our reputation depends on how our suppliers operate.

How you help: Follow supplier processes and report concerns.

10. Planning the Right Inventory

Too much stock ties up cash; too little can stop production.

How you help: Keep data accurate and follow planning processes.

Why This Matters

Risk management isn't just a leadership or audit responsibility — **it's part of how we all do our jobs well**. Spotting issues early, following processes, and speaking up helps keep our operations safe, compliant, and competitive.

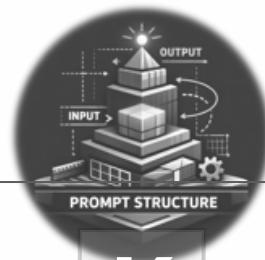
Thank you for playing your part in keeping our manufacturing operations strong and resilient.



All of these examples were created in the free Version of ChatGPT, better models would give better responses, longer, more explanatory. You get what you pay for!

- *Tone and style adapted, simpler, conversational tone.*
- *Audience centric output*

PROMPT



STRUCTURE

R O C K V O P

OUTPUT

Tell it what OUTPUT you want and in what FORMAT:

eg. "The response should be structured in bullet points with clear headings for each section. The entire response should be concise, no longer than 500 words".

Defining the output format enhances the usability of the response and ensures the structure matches your needs.

EXAMPLES

- *"Summarize the key risk factors in the company's operations **in a bullet-point format.**"*
- *"Provide an executive summary of the company's financial risk assessment in **two paragraphs and max 200 words.**"*
- *"**Create a table** outlining the top five compliance risks, including their likelihood and potential impact."*
- *"**Draft a one-page report** on operational risks, **formatted as per attached file** for inclusion in the annual risk review document."*

IMPACT ON RESPONSE

{ original prompt + }

The response should be in the form of an opening statement of the purpose of the report, no more than 40 words.

The risks should be a a table with the following columns:

- Risk Title
- Risk Description
- Impact
- Likelihood
- Mitigation Actions

Conclude the response with a summary paragraph of 30 to 50 words. Provide me also with an excel file of the table.



Opening Statement (Purpose of the Report)

This report presents an internal audit risk assessment identifying the most critical operational risks facing the company, evaluating their potential impact and likelihood, and outlining key mitigation actions to support resilient and compliant operations.

Top 10 Critical Operational Risks

Risk Title	Risk Description	Impact	Likelihood	Mitigation Actions
Global Supply Chain Disruption	Disruption to global suppliers due to geopolitical tension, pandemics, or logistics failures.	High	Medium	Diversify suppliers, maintain safety stock, and enhance supplier risk monitoring.
Manufacturing Downtime	Unexpected breakdowns or capacity constraints at UK, Poland, or China factories.	High	Medium	Preventive maintenance, capacity planning, and business continuity planning.
Quality Failures	Defects in components or finished vehicles leading to recalls or reputational damage.	High	Medium	Strengthen quality controls, audits, and supplier quality assurance.
Regulatory Non-Compliance	Failure to comply with automotive, environmental, or labor regulations across jurisdictions.	High	Low	Central compliance monitoring and regular regulatory audits.
Cybersecurity Breach	Cyberattacks disrupting manufacturing systems or compromising intellectual property.	High	Medium	Implement cybersecurity controls, regular testing, and employee awareness training.
Geopolitical Risk	Trade restrictions, tariffs, or sanctions affecting cross-border operations.	Medium	Medium	Scenario planning and alternative sourcing strategies.
Foreign Exchange Volatility	Currency fluctuations impacting costs and profitability.	Medium	High	Hedging strategies and currency exposure monitoring.
Labor Availability and Relations	Shortages of skilled labor or industrial action disrupting operations.	Medium	Medium	Workforce planning, engagement initiatives, and contingency labor arrangements.
Environmental and Sustainability Risk	Failure to meet sustainability expectations or environmental standards.	Medium	Low	Environmental management systems and sustainability reporting.
Health and Safety Incidents	Workplace accidents causing injury, shutdowns, or legal exposure.	High	Low	Robust health and safety programs and regular training.

Conclusion (Summary)

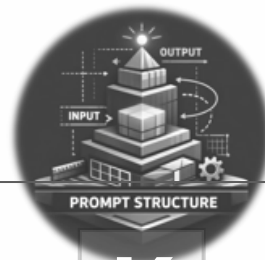
Overall, the company faces a complex risk profile driven by global supply chains, regulatory diversity, and operational concentration. Proactive risk management, strengthened controls, and continuous monitoring are essential to safeguard operational continuity, financial performance, and corporate reputation.

Excel file:

The screenshot shows an Excel spreadsheet titled "Vehicle_Manufacturing_Risk_Assessment.xlsx". The spreadsheet contains the same data as the table in the previous block. The Excel interface is visible, showing the ribbon with tabs for Home, Insert, Draw, Page Layout, Formulas, Data, Review, View, and Automate. The Home tab is active, showing options for Paste, Cut, Copy, Format, and text formatting (font face, size, bold, italic, underline). The status bar at the bottom indicates the active cell is A1, containing the text "Risk Title".

• Output format as requested!
• Opening, Closing, table and Excel file! I just need to add some formatting (but even that can be directed!)

PROMPT



STRUCTURE

R O C K V O P

PRINCIPLES

Tell it what PRINCIPLES (rules/behaviours) to follow :

eg. "Always acknowledge when information is uncertain, never present opinions as facts, and when discussing controversial topics, always present multiple viewpoints."

Guides the model on the behaviours and preferred methods to use and sequence in interaction. Eg. workflow, Critical thinking, alternatives etc.

EXPLANATION

Rules and principles can guide how the model should behave when responding. Use directive, clear, actionable rules that the AI can follow and you can verify, eg. (but not limited to)

- **Do Not** [action not to do]
- **Always** [specific behaviour you want]
- **Never** [specific behaviour to avoid]
- **When** [situation], **always** [required action]
- Describe a clear Workflow eg. Provide me with an outline and **await my response before proceeding with the detailed report. Step one is ...**

Example:

- "Always acknowledge when information you present is uncertain. Never present opinions as facts, and when discussing controversial topics, ALWAYS present multiple viewpoints."
- "Never say things like "great idea" if you don't see it as a genuinely good, and original idea" ***
- ALWAYS Tell me if you think I am wrong or have missed something. ***
- Never guess or assume, tell me you don't know.
- "Ask clarifying questions as needed."

IMPACT ON RESPONSE

Without Prompt

You are an internal auditor, write a risk assessment for a manufacturing facility that you will audit, it is located in France and is part of a 10 Billion Euro International Company that manufactures and sells industrial cooking equipment.

With Prompt

You are an internal auditor, write a risk assessment for a manufacturing facility that you will audit, it is located in France and is part of a 10 Billion Euro International Company that manufactures and sells industrial cooking equipment.

Before writing the report you must first propose an outline of the content headers and present it to me for review and agreement.

Whenever you propose an outline, always present just the headers/title of the section with a max 10 word word explanation of the content of that section.

Do Not write the report or take further actions until receiving my agreement to do so.

(Even with this always remember, all LLM's make mistakes, prompting can help but never eliminate completely)

***Principles can benefit from being placed early in a longer prompt, and even repeated at the end in very long long prompts**

***** Sycophancy is very difficult to address as it seems to be embedded, these principles altering surface behaviour only**

You are an internal auditor, write a risk assessment for a manufacturing facility that you will audit, it is located in France and is part of a 10 Billion Euro International Company that manufactures and sells industrial cooking equipment.

Without

Internal Audit Risk Assessment – Manufacturing Facility (France)

Audit Title: Operational and Compliance Audit of French Manufacturing Facility

Business Unit: Industrial Cooking Equipment Manufacturing

Location: [City], France

Audit Period: [Insert Period]

Date Prepared: [Insert Date]

Prepared By: Internal Audit Department

1. Executive Summary

This risk assessment evaluates the key risks associated with the operations at the French manufacturing facility, which plays a critical role in the production of industrial cooking equipment for an international group generating over €10 billion in revenue across both European and international markets, and its operations include manufacturing, quality control, and distribution.

2. Objectives of the Audit

- Evaluate operational efficiency and effectiveness of manufacturing processes
- Assess internal controls over production, inventory, and procurement
- Identify compliance risks with local, EU, and corporate regulations
- Review alignment with group policies on health, safety, environment, and sustainability
- Examine risk management practices and business continuity plans

3. Risk Categories and Assessment

Risk Area	Risk Description	Likelihood	Impact	Risk Rating	Mitigating Factors
Operational Risk	Production disruption due to machinery breakdown, labor shortages, or supply chain constraints	Medium	High	High	Maintenance schedules, equipment diversification, inventory buffers
Supply Chain Risk	Delays or quality issues with critical components sourced externally	Medium	High	High	Approved vendors, dual sourcing, quality checks, dual sourcing
Health & Safety	Workplace accidents or non-compliance with French labor laws and EU directives	Low to Medium	High	Medium to High	Health & safety training, regular inspections, PPE enforcement
Environmental Compliance	Breach of environmental regulations (e.g., emissions, waste disposal)	Low	High	Medium	ISO 14001 certification, regular environmental audits
Quality Risk	Defective products leading to returns, recalls, or customer dissatisfaction	Medium	Medium to High	High	Quality assurance protocols, root cause analysis, customer feedback loops
Cybersecurity Risk	Threats to manufacturing control systems or ERP through cyberattacks	Medium	High	High	IT security patches, network monitoring, employee awareness training
Financial Controls	Errors or fraud in inventory valuation, procurement, or production costing	Medium	Medium	Medium	Segregation of duties, internal reviews, regular audits
Compliance Risk	Non-compliance with corporate policies, anti-bribery laws (Sapin II), and EU regulations	Low	High	Medium	Ethics training, whistleblower hotline, compliance reviews
Business Continuity	Lack of preparedness for major disruptions (e.g., fire, strikes, pandemics)	Medium	High	High	Business continuity plan, insurance coverage, crisis simulation
Reputation Risk	Product safety issues, labor disputes, or environmental incidents impacting brand	Low to Medium	High	Medium to High	CSR initiatives, public relations planning, legal support

4. Key Focus Areas for Audit

- Effectiveness of manufacturing and quality control processes
- Compliance with local labor and environmental laws
- Inventory management and procurement controls
- Cybersecurity posture and ERP access management
- Alignment with group sustainability and ESG goals
- Vendor management and supply chain resilience
- Adequacy of health and safety practices

5. Recommended Audit Approach

- **Walkthroughs and Process Mapping:** Document and analyze key manufacturing, inventory, and procurement processes
- **Control Testing:** Test key controls over operations, compliance, and finance
- **Interviews:** With plant management, safety officer, HR, quality control, and IT
- **Site Inspection:** Evaluate safety, environmental, and physical access controls
- **Data Analytics:** Analyze production data, downtime logs, purchase orders, inventory adjustments

6. Conclusion

Given the facility's strategic role in the company's European operations and the inherent risks in manufacturing, this location warrants a **full-scope audit** with a focus on **operational integrity, regulatory compliance, and financial controls**. The audit will help ensure risks are being effectively mitigated and that the facility aligns with group-wide expectations for compliance, performance, and sustainability.

Let me know if you'd like this as a downloadable document or tailored to a specific audit type (e.g., SOX, ISO, ESG).

You are an internal auditor, write a risk assessment for a manufacturing facility that you will audit, it is located in France and is part of a 10 Billion Euro International Company that manufactures and sells industrial cooking equipment.

Before writing the report you must first propose an outline of the content headers and present it to me for review and agreement.

Whenever you propose an outline, always present just the headers/title of the section with a max 10 word word explanation of the content of that section.

Do Not write the report or take further actions until receiving my agreement to do so.

Exerting control of the scope and structure of the response – putting yourself in the development loop!

Here is the proposed outline for the **Risk Assessment Report** of the manufacturing facility in France:

1. Executive Summary

High-level overview of key findings and conclusions.

2. Audit Scope and Objectives

Defines boundaries, purpose, and audit goals.

3. Facility and Organizational Overview

Basic details about location, structure, and business operations.

4. Risk Assessment Methodology

Approach used to identify, assess, and prioritize risks.

5. External Environment Risks

Macroeconomic, regulatory, and geopolitical factors.

6. Operational Risks

Production, supply chain, maintenance, and capacity.

7. Health, Safety, and Environmental (HSE) Risks

Risks related to employee safety and environmental impact.

8. Financial and Compliance Risks

Financial reporting, fraud, and regulatory compliance exposures.

9. Information Technology and Cybersecurity Risks

IT infrastructure, data protection, and system vulnerabilities.

10. Human Resources and Labor Risks

Staffing, labor laws, and union relations considerations.

11. Strategic and Reputational Risks

Brand impact, competition, and long-term viability issues.

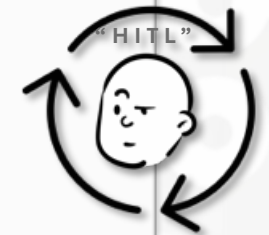
12. Risk Rating Summary and Heat Map

Visualization and ranking of identified risks.

13. Recommendations and Next Steps

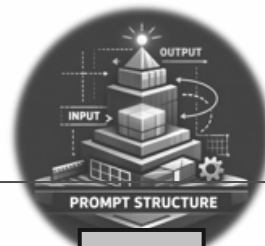
Actionable suggestions to mitigate or monitor risks.

Please review and let me know if you approve this outline or would like to make any adjustments.



PROMPT

STRUCTURE



KNOWLEDGE

Give it / point it to specific KNOWLEDGE to use in preparing its response:

Specify method, standard, framework to apply if appropriate.

If specialised or bespoke then detail it in the prompt or add a document that contains it.

Often added into GPT'S, Gems or added in skills, but also simply added to prompts. Characterised by something that is constant (just update when revised or new version released)

EXAMPLES

Apply [*Primary Professional Standard Name + Version*] - specifically [*Section/Principle Reference*]
Confirm you are using the [*Current Version Date*] version, not the superseded [*Previous Version*]


Evaluate against [*Framework Name + Version*] – all components.
Map findings to specific [*Framework*] principles where applicable

Follow the attached Internal Audit Methodology (v3.2) document for finding documentation <add the file in the prompt>
Apply the Risk Rating Matrix (provided) for severity assessment <add the file in the prompt>

- Verification**
- Copyright/permissions allowing, add the specific documents to the prompt of tool knowledge base.
 - Before responding, confirm which version of each framework you are referencing
 - If any framework version is uncertain, state this explicitly
 - If the referenced knowledge is not in the public domain and you cannot get full access to it state this explicitly.
 - Cite specific section/standard numbers when referencing framework requirements

• *SEE PRINCIPLES IN FIRST PROMPT EXAMPLE* PF_P2

IMPACT ON RESPONSE

 HG_Movement_Risk_Assessment_... Document

Act as an internal auditor, conduct a risk assessment of the top 10 most critical risks in the operations of a medium sized vehicle manufacturing company called HG Movement.
The company has assembly factories in the UK and Poland, and a components fabrication factory in China. The company sources other key components and parts from suppliers across the world. The risk assessment methodology and process to use is the HG Movement Risk Assessment Methodology. This methodology is described in the attached file:
HG_Movement_Risk_Assessment_Methodology_Policy.docx
You MUST follow this methodology precisely.
Ask clarifying questions.
Offer your assistance in the preparation steps and guide the user through the process step by step.
YOU MUST start your response with a checklist of the key steps as described in sections 6 and 7 of the methodology. You MUST always explain what step we are undertaking and when prompted provide the user with a status update against the required steps.

<Knowledge File also includes "Output" Guidance>



HG_Movement_Risk_Assessment_...
Document

Added the "knowledge" file

Can add multiple files eg.
Another file with more context!

<Role & Objective>

Act as an internal auditor, conduct a risk assessment of the top 10 most critical risks in the operations of a medium sized vehicle manufacturing company called HG Movement.

<Context>

The company has assembly factories in the UK and Poland, and a components fabrication factory in China. The company sources other key components and parts from suppliers across the world.

<Knowledge>

The risk assessment methodology and process to use is the HG Movement Risk Assessment Methodology. This methodology is described in the attached file:

HG_Movement_Risk_Assessment_Methodology_Policy.docx

Referenced the "knowledge" file *(belt & braces)*

<Principles>

You MUST follow this methodology precisely.

Ask clarifying questions.

Offer your assistance in the preparation steps and guide the user through the process step by step.

YOU MUST start your response with a checklist of the key steps as described in sections 6 and 7 of the methodology. You MUST always explain what step we are undertaking and when prompted provide the user with a status update against the required steps.

Added Principles to work to!

✓ **HG Movement Risk Assessment – Methodology Checklist (Sections 6 & 7)**

Below is the **mandatory checklist of key steps** we must follow **exactly** as defined in Sections 6 (Preparation) and 7 (Execution) of the *HG Movement Risk Assessment Methodology*.

I will reference this checklist throughout and provide **status updates** as we progress.

Section 6 – Key Preparation Steps

1. Define assessment **scope, objectives, and timeframe**
2. Confirm **stakeholders and participants**
3. Gather **background information and data**
4. Identify **key processes and assets** in scope
5. Select **risk rating model** and confirm **risk appetite thresholds**
6. Prepare **templates** (risk register, heat map, report)
7. Schedule **workshops/interviews** and issue pre-reads

Section 7 – Execution Steps

8. Identify risks
9. Define risk statements and categories
10. Assess inherent risk (likelihood & impact)
11. Identify and evaluate key controls
12. Assess residual risk
13. Determine risk responses and action plans
14. Validate, finalize, and identify **Top 10 risks**

🔍 **Current Step We Are Undertaking**

Step 6.1 – Define the assessment scope, objectives, and timeframe

Before I can credibly identify and rank the **Top 10 most critical operational risks**, I must first **define the scope and assumptions**. This is a **mandatory prerequisite** under the methodology.

❓ **Clarifying Questions (Required to Proceed)**

Please answer the questions below. I will not advance to risk identification until the line with the policy.

1. Scope Confirmation

Do you want this risk assessment to be:

- **Enterprise-wide operational risk assessment** (covering all major operations)
- **Operations-focused only**, limited to:
 - UK Assembly
 - Poland Assembly
 - China Components Fabrication
 - Global Supply Chain & Logistics

Note: Your request mentions "operations," but the methodology requires us to explicitly confirm the scope boundaries.

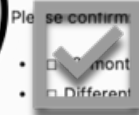
2. Objective of the Assessment

What is the **primary purpose** of this assessment? (Select all that apply)

- Input to **Audit Committee / Board** reporting
- Input to **Internal Audit annual plan**
- Management operational risk prioritization
- Regulatory / governance requirement
- Scenario planning / resilience testing

3. Time Horizon

Unless otherwise specified, the methodology defaults to **12 months**.



- **12-month forward-looking assessment** (default), or
- **Different horizon** (please specify)

Risk Appetite & Escalation

Can we assume the **standard HG Movement escalation thresholds** apply?

- High risk = score **10–16** → ELT & Audit Committee
- Extreme risk = score **17–25** → Immediate ELT & Audit Committee
- Yes, use standard thresholds
- No, appetite differs (please explain)

5. Stakeholder Assumptions

If not specified, I will assume the following **risk owners** for operational risks:

- Manufacturing: Plant Directors (UK, Poland, China)
- Supply Chain: Global Procurement / Supply Chain Director
- Quality: Global Quality Director
- IT/OT: CIO / Head of OT
- H&S: Global HSE Lead
- Confirm assumptions
- Provide alternatives

🕒 **How I Will Guide You (Step-by-Step)**

Once you respond:

1. I will **lock the scope and assumptions** (Step 6.1–6.2)
2. Guide you through **process & asset identification** (Step 6.4)
3. Facilitate **structured risk identification** aligned to HG objectives (Step 7.1)
4. Build a **Top 10 operational risk register** with:
 - Proper risk statements
 - Inherent & residual scoring
 - Control effectiveness assessments
 - Clear rationale (as required by Section 10)
5. Conclude with:
 - Top 10 risk summary
 - Heat map positioning
 - Escalation status
 - Suggested Internal Audit focus areas

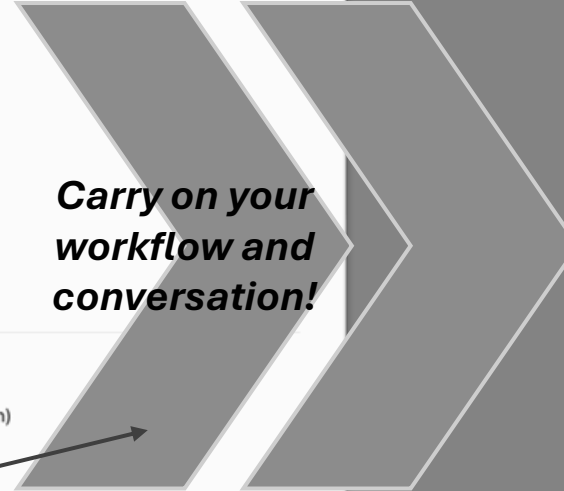
🕒 **Status Update (Against Methodology)**

- **Preparation Steps:** 🟡 *In progress* (awaiting scope confirmation)
- **Execution Steps:** 🟠 *Not yet started – per policy requirements*

Please respond to the **clarifying questions above**, and we will proceed immediately to the next required step.



*Check the methodology
Is being followed.*



Session Three:

Prompting Strategies for improving results!

... But remember mistakes are still made , HITL is still needed.

Don't forget

Prompting is not a panacea for all ill's

Prompting and prompting strategies are only ever a guide, a steer, always open to interpretation, it is never a hardwired command or immutable set of deterministic rules. It does not circumvent the probabilistic nature of these models out put.

Good prompting and other skills can improve the quality of response but never eliminate the chance of "hallucination", which is in fact a feature of the systems design rather than a bug!



An auditor's arsenal for improving quality is always evolving

Your Critical Mind: GIAS 4.3 Professional Skepticism

Understanding how these models actually work!

What they are good at, what they are not good at.

Good Prompting practices

Verification built into you work-flows (HITL).

Other suggestions ...?



Two Prompting Paths: Creative & Structured

Creative Path

When to use: Explore, brainstorm, generate options, learn new things:

- Looser, vaguer prompts
- Less constraint on principles and context
- Invite AI to surprise you
- Some outputs won't be useful – that's fine

Structured Path

When to use: Know what you want, need specific context and boundaries:

- Detailed, specific prompts
- Clear constraints and principles
- Explicit quality criteria
- Less room for AI interpretation
- Constrain sources

- *Evolve : Start creative, finish structured – explore first, then constrain for delivery*
- *I work with it in a fluid way, depending on the task or objective hand. Moving from path to path.*
- *Always mindful of if AI is the right tool for the task, sometimes it can take longer trying to steer and guide and re-iterate, you will learn where and how to start, and even if to start as your fluency grows.*

(Even with this always remember, all LLM's make mistakes, prompting can help but never eliminate completely)

Does order of the prompt matter?

- Lot's of practioner discussion, some technical papers around the "lost in the middle" effect in large contextual retrieval.
- **Clear structure**, delimiters, parsing, spaces, emphasis is seen as being important to help models understand large prompts.
- Making sure your instructions and prompt elements **do not contradict themselves** is also very good practice.
- Current "wisdom" points to order being **less important in shorter prompts and more important in long prompts** with lots of context eg. Either text or added files.
- **Repeating non negotiables (principles)** in long prompts (beginning and end) is seen as good practice.
- Mental model I use for long prompts:
 - **EDGES (beginning and end) : Control Planes** (what to do, how to format, what not to do)
 - **MIDDLE: Data Plane** (the stuff to draw from)

Response Critiquing Strategies

1. Ask for Pros and Cons

Get AI to argue the other side of its own recommendation

"You've suggested X. Now give me the strongest arguments against X."

2. Request Alternative Options

Don't settle for the first answer – compare options

"Give me three different approaches with the trade-offs of each."

3. Challenge the Response

Ask AI to find flaws in its own output

"Look at what you just produced. What's wrong with it?"

"Prove your answer is right"

4. Ask "Why Am I Wrong?"

Stress-test your own conclusions before committing

"I'm thinking that [conclusion]. Tell me why I might be wrong."

5. Test with Different Framing

Same question, different angle – check for consistency

"What are the key risks?" then "How would you commit fraud here?"

6. Verify Sources and Citations

Always check – hallucinated citations are common

"I always follow and test some links, because sometimes they're not correct."

Warning: AI can create an infinite loop of arguments for and against if you ask it to!

(Even with this always remember, all LLM's make mistakes, prompting can help but never eliminate completely)

Using Principles to shape behaviour and results

The Challenge

- When you find recurring issues with AI outputs, address them through explicit principles – rules that govern how AI should behave. These become part of your prompt, or custom/gpt instruction, creating guardrails for more consistent results. Make them **MANDATORY!**

Eg: Mermaid Problem (*Mermaid: A text-based diagramming language that generates flowcharts from simple code syntax*)

- Some LLM's consistently generates Mermaid flowchart code with syntax errors – parentheses in labels, overly long lines, untested output that fails to render.

Applying a 4-Step Pattern solution!

1. **Identify:** Noticed Mermaid code failing repeatedly
2. **Diagnose:** Pinpointed specific failure modes (with models help)
3. **Create:** Wrote explicit rules addressing each
4. **Verify:** Built in mandatory checklist requirement into the prompt, instructing the LLM to self audit it's output.

The Resulting Principle

(Even with this always remember, all LLM's make mistakes, prompting can help but never eliminate completely)

Understand the Sources of LLM Responses

1. It's Training

What the model "learned" during training – strongest for well-established topics, has a cut-off date may be 12/18 months earlier

2. Information You Provide in Chat (Context & Knowledge)

Your prompts, context, and details – only as reliable as what you share

3. Web Search Results

Real-time information if enabled – but AI summarises, introducing more potential error in addition weak source. Paywalls also stop AI!

4. Uploaded Files & Documents (Context & Knowledge)

AI reads what you upload – may miss nuances or misread complex formatting

5. Instructions

Projects, Custom Instructions, or configured settings shaping responses

6. Hallucinations !

Not a real source. AI predicts the "next likely word", generating plausible-sounding content that isn't grounded in anything

Most advanced models will list and link the sources they have used automatically or if prompted BUT - Sometimes they can be fictitious – remember you are the HITL and quality control.

(Even with this always remember, all LLM's make mistakes, prompting can help but never eliminate completely)

Building Verification Into Your Workflow

The Problem

- Asking AI to produce complete deliverables in one go makes errors harder to spot and fix. Verification shouldn't be an afterthought, it should be built into how you work. Be an interactive editor and contributor!

Chunk Your Work

- Break tasks into stages with natural review points
- Review, adjust, and course-correct along the way

"Present your proposed structure first and wait for my approval before proceeding"

The Verification Rhythm

- **Before:** What response do you expect? How will you verify it?
- **During:** Watch for surprising, specific, or consequential claims
- **After:** Allocate verification time proportionate to the stakes.

Tip: Start with topics you are an SME in!

(Even with this always remember, all LLM's make mistakes, prompting can help but never eliminate completely)

When You're Stuck: Ask AI

When you're struggling to write an effective prompt, ask AI to help you write it.

Use the tool intelligently.

Example Prompts you could try:

"I need to create a prompt that will help me [describe your goal]. The output should [describe what you need]. What information should I include in my prompt to get a good result?"

"I'm trying to get an LLM to [describe the task], but my results aren't quite right. Here's what I've been asking: [your current prompt]. How could I improve this?"

(Even with this always remember, all LLM's make mistakes, prompting can help but never eliminate completely)

Session Four:

Model Features that Steer Responses

Beyond the Chat Box

Platform Features for Internal Auditors

Not exhaustive and new features coming all the time eg. Claude Cowork!

Model features and tools can elevate you “AI Game”!

- Good prompting is fundamental and where we start, but also
- Understanding what models to choose, which version to work in, how to build persistence through memories (and when to switch them off) , custom behaviours, instruction, project flows, custom agents !
- ... these can make integrating AI into to you day to day workflows and tasks more effective.
- **It’s a probabilistic system**, it will never be right all the time, the **HITL is always essential**, but
- Combining good prompts, with it for the right things, with the right strategies, and customising your workspace will help you be more in control of what's happening!

Beyond the Chat Bot - 1

CHOOSING DIFFERENT MODELS

- **What it does:** Select from multiple AI models with different capabilities — faster/lighter models for simple tasks, more powerful models for complex reasoning, and specialised "thinking" modes for multi-step problems
- **Benefits:** Match model to task complexity; save time & resources on routine queries; deeper reasoning when stakes are higher
- **Watch outs/Risks:** More capable models aren't always better — they may over-elaborate simple requests; model availability and features vary by subscription tier; "thinking" modes cost more and take longer, so use deliberately.

ACTIVATING WEB SEARCH

- **What it does:** Enables the model to search the internet in real-time, retrieving current information beyond its training cut-off date
- **Benefits:** Up-to-date regulations, guidance, news, and industry developments; find recent publications and announcements
- **Watch outs/Risks:** AI summarises search results — potential misinterpretation; it's the internet!; paywalled content can't be retrieved; always cross-reference important findings independently. Prompt injections from unsafe websites and content.

TONE & STYLE CUSTOMISATION

- **What it does:** Configure your preferred communication style (formal, concise, detailed, etc.) in platform settings so it applies automatically without repeating in every prompt
- **Benefits:** Consistent tone & Style across output; reduces repetitive prompting
- **Watch outs/Risks:** Style settings may conflict with prompt-level instructions, causing unpredictable results; overly rigid style constraints can reduce response quality on varied tasks; review settings periodically — forgotten preferences can bias outputs

⚠ Model features and tools are changing all the time, added to, removed – weekly, monthly!

⚠ Model features & tools can carry specific risks in respect of security, access & data exfiltration, and require organisational testing and approval, understand what you are activating!

⚠ Models drift, evolve and change, this impacts their interpretation and response to prompts and instructions – build in rigor around regular testing and monitoring.

Beyond the Chat Bot - 2

DEEP RESEARCH MODES & ANALYST MODES

- **What it does:** Conducts extended, multi-step research across multiple sources, synthesises findings, and produces structured reports with citations.
- **Benefits:** Thorough investigation of complex topics; citations provide verification starting points; useful for emerging risks, regulatory changes, or pre-audit research etc.
- **Watch outs/Risks:** Resource-intensive — reserve for tasks warranting depth; citations still require verification (AI may misrepresent sources); can produce lengthy outputs that need critical editing;

PROMPT LIBRARIES (Copilot)

- **What it does:** Save effective prompts for quick reuse; share standardised prompts across your team via a central gallery.
- **Benefits:** Consistency across team members using approved prompts; time savings by not recreating effective prompts; institutional knowledge capture of what works
- **Watch outs/Risks:** Saved prompts can become stale as AI capabilities evolve; sharing prompts may inadvertently share sensitive context; prompts that work for one user may not suit another's needs.

INTERACTIVE WORKSPACES: CANVAS / ARTIFACTS / PAGES

- **What it does:** Opens a separate, editable, downloadable workspace alongside chat where you can directly explore and modify AI-generated content without changing the rest of the response (that's in the canvas. See live renderings of code (Claude/CoPilot)
- **Benefits:** Collaborative and selective editing without losing chat context; immediate visual feedback on code and diagrams; iterate on deliverables in-place rather than copy-pasting
- **Watch outs/Risks:** Features vary significantly across platforms (ChatGPT Canvas ≠ Claude Artefacts); rendered code/apps may have errors — test before relying on outputs; workspace content may not persist between sessions depending on platform;

⚠ Model features and tools are changing all the time, added to, removed – weekly, monthly!

⚠ Model features & tools can carry specific risks in respect of security, access & data exfiltration, and require organisational testing and approval, understand what you are activating!

⚠ Models drift, evolve and change, this impacts their interpretation and response to prompts and instructions – build in rigor around regular testing and monitoring.

Beyond the Chat Bot - 3

CUSTOM INSTRUCTIONS

- **What it does:** Set persistent instructions (elements of ROCKVOP) that apply automatically to all new chats — defining your role, crinciples , Tone, Output etc without repeating them each time
- **Benefits:** Consistent behaviour aligned to your methodology; reduced repetitive prompting; can be tailored per Project for engagement-specific requirements
- **Watch outs/Risks:** Instructions can conflict with individual prompts unpredictably; complex or contradictory instructions cause inconsistent behaviour; forgotten instructions may bias outputs in ways you don't notice; review and update periodically. Switch on / off.

MEMORY

- **What it does:** The model retains information from previous conversations to personalise and contextualise future interactions — learning your preferences, projects, and working context over time
- **Benefits:** Reduced need to re-explain context; increasingly tailored responses as the model learns your work; continuity across sessions
- **Watch outs/Risks: Memory introduces bias** — past context influences current responses, which may not be appropriate for every task; retained information may become stale or incorrect; sensitive information in memory creates data exposure; know how to view, edit, and disable memory; consider turning off for fresh-perspective tasks

PROJECTS (Notebooks in CoPilot)

- **What it does:** Creates dedicated workspaces ("smart containers") that keep related chats, uploaded files, and custom instructions together — maintaining persistent context across a longer effort such as an audit engagement.
- **Benefits:** Maintain project context; centralised knowledge base (policies, prior reports, standards); consistent behaviour via project-level instructions; can leave and come back to it.
- **Watch outs/Risks: Stale context** — old documents remain unless removed; having documents "available" doesn't mean AI interprets them correctly; conversations within a project are still separate (AI doesn't see other chats unless memory is enabled); document upload limits vary by platform; instruction drift can cause inconsistent behaviour over time; manitain the knowldege library

⚠ Model features and tools are changing all the time, added to, removed – weekly, monthly!

⚠ Model features & tools can carry specific risks in respect of security, access & data exfiltration, and require organisational testing and approval, understand what you are activating!

⚠ Models drift, evolve and change, this impacts their interpretation and response to prompts and instructions – build in rigor around regular testing and monitoring.

Beyond the Chat Bot - 4

CUSTOM GPTs, DECLARATIVE AGENTS, GEMS

- **What it does:** Create or use pre-configured AI assistants with specific instructions, knowledge bases, tools, and focus areas — designed to repeatedly help with particular task types (e.g., "Finding Drafter", "Root Cause Assistant")
- **Benefits:** Purpose-built tools without configuring from scratch each time; shareable across teams; can include specialised knowledge and workflows
- **Watch outs/Risks: Agent drift** — agents may deviate from instructions over extended interactions; embedded instructions can introduce bias; third-party/public agents may have undisclosed instructions or data handling; knowledge bases can become outdated; security review required before deploying agents with access to sensitive data or systems connections or plug ins etc. Model drift and interpretation risk.

NUMERICAL ANALYSIS, CALCULATIONS, GRAPHS & CODE WRITING

- **What it does:** AI writes and executes code to perform calculations, analyse data, and generate charts/visualisations in execution tools it has access to — moving beyond text prediction to computation. It can also write code for applications.
- **Benefits:** Mathematical operations (unlike pure language models); data analysis of uploaded files; visual outputs for reports and presentations. Building your own small apps.
- **Watch outs/Risks:** Verify the logic, not just the output — code can contain errors; large datasets may not process fully – there are better tools for large Analytics ; sensitive data uploaded for analysis creates confidentiality exposure; it writes code that can execute actions — be cautious with code from untrusted sources or that handles sensitive data, read and write access etc. **There can be significant Security issues with VC produced code – technical oversight and testing is essential.**

⚠ Model features and tools are changing all the time, added to, removed – weekly, monthly!

⚠ Model features & tools can carry specific risks in respect of security, access & data exfiltration, and require organisational testing and approval, understand what you are activating!

⚠ Models drift, evolve and change, this impacts their interpretation and response to prompts and instructions – build in rigor around regular testing and monitoring.

SESSION 6

Internal Audit Centric Use Cases

For Personal Use Only
All rights reserved.

USE CASES

We'll cover what time permits!

1. Research
2. Report Formats - Creating Fixed Formats
3. Process Walkthrough Flow Chart & Test Plan
4. Audit Report Communication CoPilot Agent
5. Vibe coding an interactive Risk Map App

For Personal Use Only
All rights reserved.

A Little Research?

WHAT: Use the model you explore issues and risks in a potential Audit Area , also look for similar entities elsewhere and outside the company and to comment on planned scope.

TIP: RESEARCH MODES are becoming increasingly powerful and customisable in all models.

For example CoPilot RESEARCHER AGENT allows you to actively choose sources:



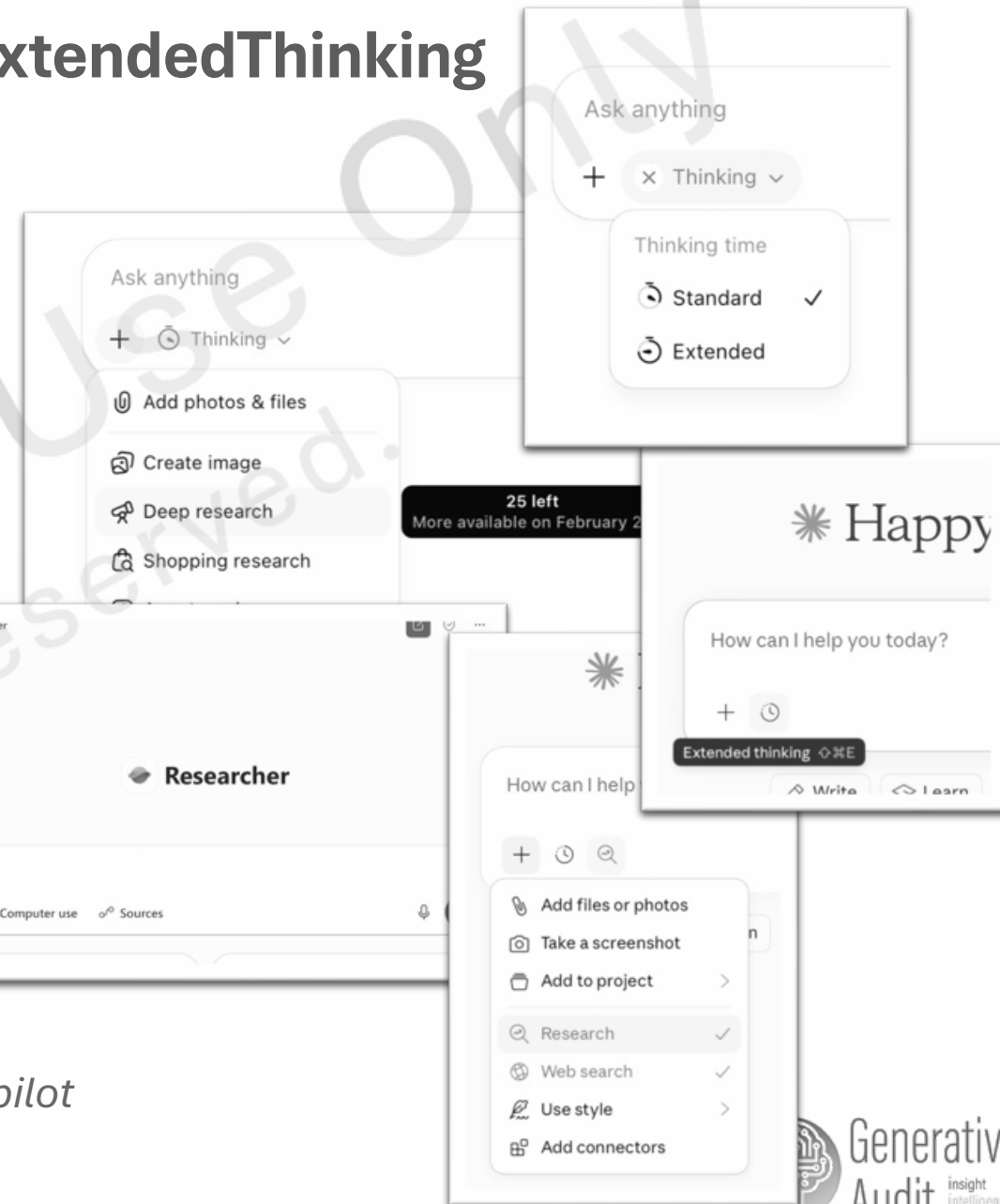
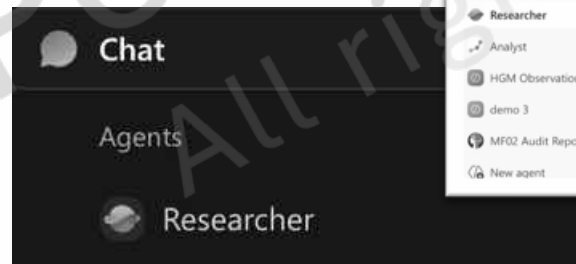
HOW:

- Used CoPilot Standard conversation (GPT5 on) and also tried with Research Agent.
- A prompt to research risks and examples of failures in similar companies.
- This can help in engagement and work planning, may also serve to reiterate scope.
- **NB: This could be improved by “Chunking / Chain Prompting” or breaking the prompt into steps.**

Expanding What AI Can Do: Research & Extended Thinking

Deep Research & Extended Thinking

- Spends more time processing before responding
- Conduct thorough research across multiple sources
- Apply more rigorous reasoning to complex problems
- **⚠ Caution:** Takes longer and may use more resources — use for tasks that warrant depth



Deep Research available on Claude, ChatGPT, Gemini, and Copilot

Report Formats (easy way)

WHAT: Create a Formatted Report template in word that can be added to a prompt, project or Agent to create repeatable output.

USE CASE
Demo F1



DEMO F1

HOW: Create a word (or excel) file with the desired structure, format and [instructions] as a “wire frame”:

- **Instructions (Prompts) in the template:** These instruct the LLM what to do in that part of the template.
- **Use of [...] :** Directs the LLM to recognise what is written within as an instruction.
- **Use MS Styles:** These embed markers so you can easily apply Designs to files produced by the model

Walkthrough Flow Charting & Test Plan

WHAT: Use Claude (or ChatGPT) to evaluate an interview transcript, convert it into a process flow chart, and plan a control testing.

USE CASE
Demo W+FC



DEMO W+FC

HOW: Use the interpretive and code writing capabilities in eg. Claude or ChatGPT to assess and visualise a process walkthrough

1. Prepare Interview transcript (could be from a recorded meeting!)
2. Ask model to summarise and describe process
3. Ask model to create mermaid code for a process flow chart based on the walk through.

4

An Audit Report Communication Agent

WHAT: Instead of sending an audit report, give access to an agent that has the Audit Report, Company Policies and Company Controls as knowledge

USE CASE
CoPilot



HOW: Configure a CoPilot Agent as follows:

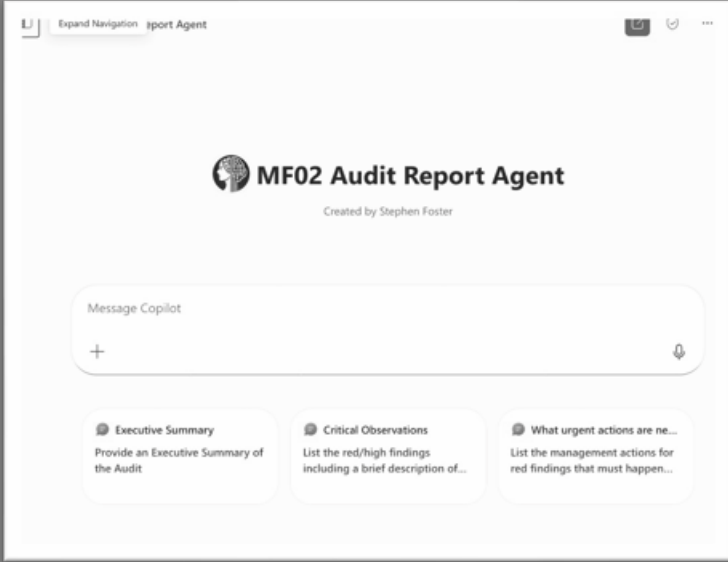
- **Instructions:** How to respond, confirm role of user, how to respond to policy questions.
- **Knowledge:** Full Audit report and findings, GRC Evaluation, Policies and Controls
- **Share the CoPilot Agent:** Distribute to all recipients of Audit Report

DEMO AGENT:



MF02 Audit Report Agent

Chat Interface



Example chat

Provide an Executive Summary of the Audit

MF02 Audit Report Agent

Here is the Executive Summary from the internal audit of MF02 (Berlin Production Facility), as documented in the **MF02 Full Audit Report 2025**:

Executive Summary – Internal Audit of MF02 (Berlin Production Facility)

Audit Reference: KRP010124

The audit, conducted in June 2024, focused on operational resilience, compliance, and control effectiveness across key risk areas: production, supply chain, health and safety, cybersecurity, third-party management, and anti-fraud controls.

Overall Rating: RED – Urgent Improvement Needed

This rating reflects eight Red-rated observations, including:

- **Production Planning:** Inconsistent adherence to Sales & Operations Planning (S&OP) and Master Production Schedule (MPS).
- **Supply Chain Risk:** Over-reliance on single-source suppliers without contingency or dual sourcing.
- **Inventory Control:** Accuracy issues with >10% variances and poor tracking of work-in-progress (WIP) and scrap.
- **Health & Safety:** Expired or missing training records, managed manually via spreadsheets.
- **Cybersecurity (OT):** Weak access controls, including shared and outdated accounts.
- **Third-Party Management:** Incomplete contractor vetting before site access.
- **Procurement Controls:** Segregation-of-duties conflicts, enabling full process control by individuals.
- **Audit Follow-up:** Incomplete implementation of 2022 audit actions, with no formal tracking or escalation.

Additional Medium-Rated Observations

These include gaps in quality documentation, maintenance backlog, environmental compliance, CSRD/ESRS readiness, disaster recovery testing, and whistleblower awareness.

Positive Response and Corrective Actions Underway

MF02 leadership has taken constructive steps, including:

- Launching a structured monthly S&OP cycle with executive oversight.
- Fast-tracking dual sourcing for critical components.
- Rolling out a Learning Management System (LMS) for safety training.
- Strengthening OT access controls and removing shared accounts.
- Centralising contractor management and procurement access reviews.
- Revalidating and tracking all open actions from the 2022 audit.

These actions are well-targeted and, if delivered on time, are expected to reduce key risks significantly. Early improvements are anticipated in the next quarter.

Let me know if you'd like a breakdown of the Red-rated observations, timelines for corrective actions, or your role-specific responsibilities.

I am the ITP process owner at MF02, I need to know the most urgent actions and then the next 6-12 months

MF02 Audit Report Agent

Thanks, Stephen. As the ITP (Invoice-to-Pay) process owner at MF02, you are not directly named as an action owner in the audit report. However, your role is critical to addressing several high-risk observations, especially those involving procurement controls, vendor risk, exception handling, and system integrity.

Here's a breakdown of what you should focus on:

Urgent Actions (Next 4–8 Weeks)

These are high-priority areas where your leadership is essential:

1. Procurement Segregation of Duties

- **Issue:** Individuals can control the full procurement cycle (requisition to payment), creating fraud risk.
- **Your Role:**
 - Review current ITP access rights and workflows.
 - Work with IT/OT and Procurement to enforce role-based access and approval limits.
 - Ensure no single user can raise, approve, and receive POs or process payments.

2. Unusual Vendor Transactions

- **Issue:** ERP exception reports (e.g. duplicate invoices, round-sum payments) are not reviewed promptly.
- **Your Role:**
 - Collaborate with Finance to define ownership and SLAs for exception resolution.
 - Ensure ITP process includes timely review and escalation of flagged transactions.
 - Support KPI tracking for investigation timeliness and resolution.

3. Contractor Due Diligence

- **Issue:** Contractors are allowed on site without full vetting.
- **Your Role:**
 - Ensure that ITP processes do not allow payment or onboarding of contractors without completed due diligence.
 - Align with Procurement and EHS on system controls and checklist enforcement.

Medium-Term Actions (6–12 Months)

These are foundational improvements that will strengthen ITP controls and resilience:

1. Audit Action Tracking

- **Your Role:**
 - Ensure ITP-related actions from the 2022 and 2024 audits are tracked in the central system.
 - Confirm closure evidence is documented and validated by Internal Audit.

2. Supplier Risk Management

- **Your Role:**
 - Support integration of supplier risk scores into ITP workflows (e.g. block high-risk vendors from

Wrap Up



Explored the AI Mindset & Sophistication of Use



A look at tools and features and a tour of CoPilot Chat



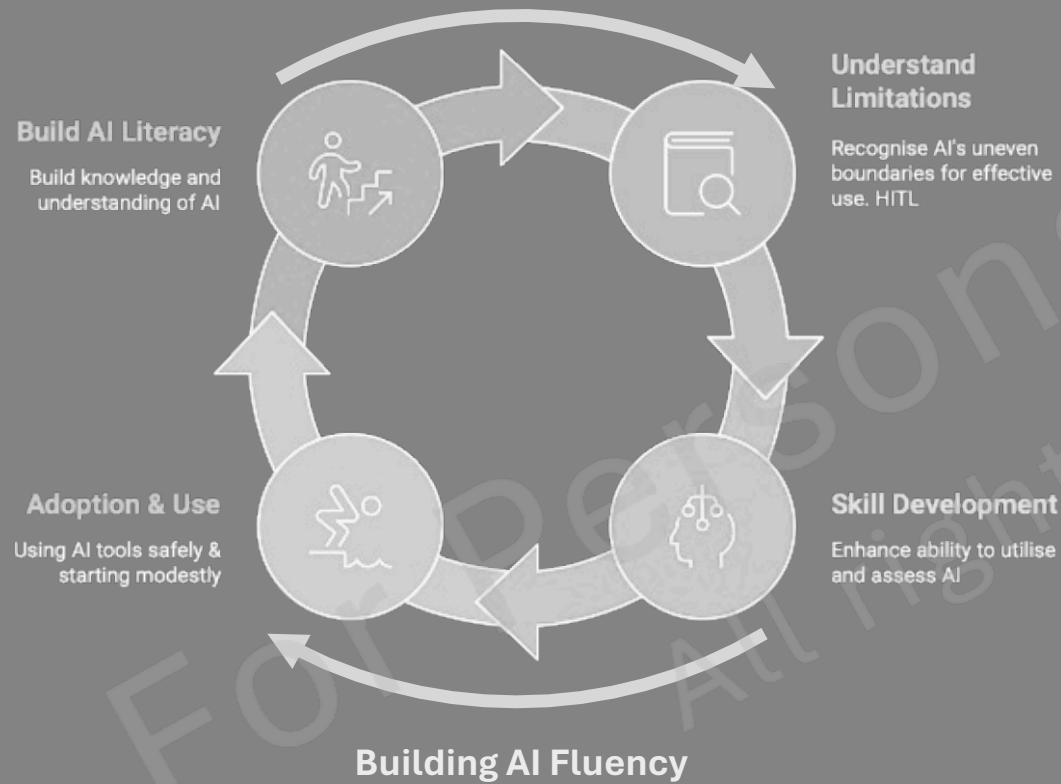
Learned how to build good prompts and prompt strategies



Explored a few augmentation use cases if we had time

Steps your ongoing journey

Continuous Learning Loop



FOUNDATIONS of AI	AI in PRACTICE	ETHICS & GRC in AI	HUMAN OVERSIGHT & LEARNING
1 Introduction to Artificial Intelligence A foundational overview of AI's basic concepts, history, and real-world applications across various sectors to build fundamental understanding.	3 Practical AI Skills & Opportunities Hands-on experience with AI tools to build practical competency, complemented by awareness of what's possible.	5 Ethical and Societal Implications Understanding the moral dimensions, potential biases, and ethical frameworks designed to ensure responsible development and deployment.	7 Human-AI Interaction A Framework for effective collaboration between internal auditors and AI systems, considering critical thinking and understanding how to adapt to the new work space.
<input type="checkbox"/> What is AI? <input type="checkbox"/> Other <input type="checkbox"/> Other	<input type="checkbox"/> Prompting <input type="checkbox"/> Other <input type="checkbox"/> Other	<input type="checkbox"/> Biases, Discrimination, manipulation <input type="checkbox"/> Other <input type="checkbox"/> Other	<input type="checkbox"/> HITL <input type="checkbox"/> Other <input type="checkbox"/> Other
2 Core AI Concepts Essential technical knowledge covering machine learning, neural networks, and data privacy principles that form the building blocks of AI systems.	4 AI & Auditing Assessment of AI use & AI systems. Dependent on extent of development, deployment and use this may encompass bias detection, explainability, technical performance, and organisational use and governance.	6 AI Risk & Governance Understanding of AI-related risks, compliance requirements, and governance structures needed to manage AI systems effectively.	8 Continuous Learning and Adaptation A active commitment to ongoing education and staying current with AI developments to maintain relevant knowledge and skills in a rapidly evolving field.
<input type="checkbox"/> Machine Learning Basics <input type="checkbox"/> Other <input type="checkbox"/> Other	<input type="checkbox"/> Auditing AI <input type="checkbox"/> Other <input type="checkbox"/> Other	<input type="checkbox"/> AI Related Risks <input type="checkbox"/> Other <input type="checkbox"/> Other	<input type="checkbox"/> Keeping pace with change <input type="checkbox"/> Other <input type="checkbox"/> Other



- We should not wait to start using it.
 - No matter how simple the first steps.
- It will be part of our future.
 - We need to make it a good part.
- But it is only a means to an end.
- Internal auditing is what we are about.

**Independent
Objective
Natural Critical Thinkers**

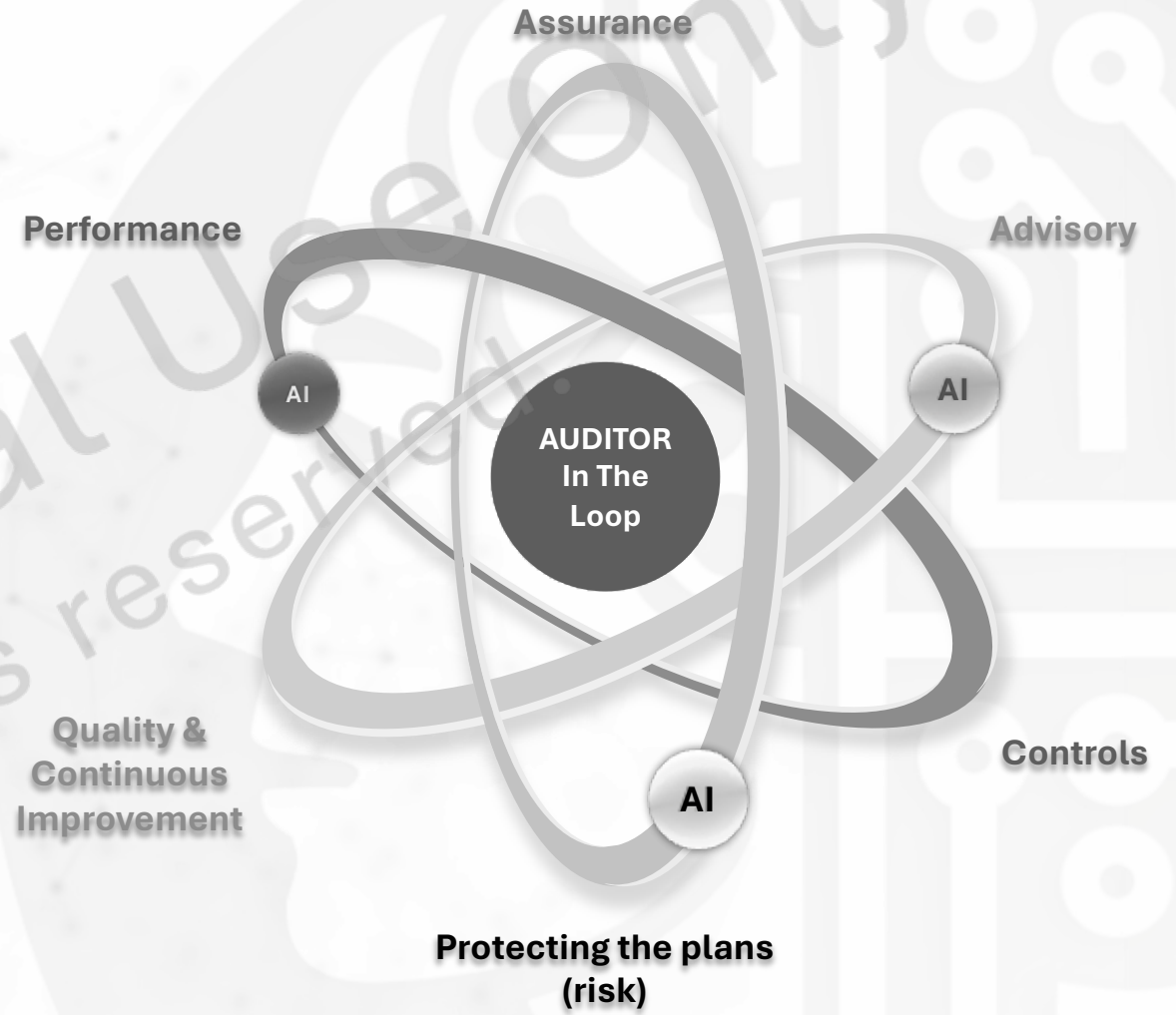
- So perhaps we are

..... the perfect

“ HITL ”



... Or even





FEEDBACK & QUESTIONS?

For Personal Use Only
All rights reserved.

THANKS FOR PARTICIPATING

Stay connected:



[linkedin.com/in/stephenfosterga](https://www.linkedin.com/in/stephenfosterga)



stephen@generativeaudit.com

