

Webinar Housekeeping

- All attendee cameras and mics are off.
- The webinar is being recorded.
- Drop your questions in the Q&A box.
- Engage with Polls!



Agenda



GenAl Intro



Prompting Techniques and Practical Tips



Use Cases & Examples



Safe AI Use



Webinar Goals

- Help legal professionals improve the way they use Al through better prompting.
- Go beyond "Summarize by Document."
- Share practical techniques.



Hello!



Jean Yang

VP AI Transformation & G2M



Mickala Anderson

Al Program Manager



Onit

Onit is a global leader of legal-related, smart workflow solutions across the enterprise: legal, compliance, sales, procurement, IT, HR and finance departments.

3,000+

Corporate customers

650+

ELM customers

24/7

Call center support

13,500+

Law firm customers

1,000+

Contracts customers

ΑI

Center of excellence

London Frankfurt Pune Auckland



Atlanta, HQ San Francisco Austin





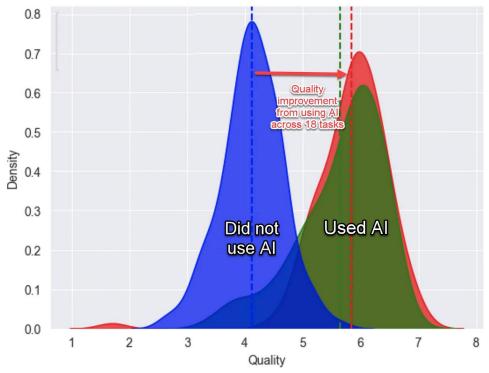


Poll Question One:

How would you describe your experience level with prompting AI tools (like ChatGPT, Copilot, etc.)?



Work is changing People + generative Al outperform just people



Navigating the Jagged Technological Frontier: Field Experimental Evidence of the Effects of AI on Knowledge Worker Productivity and Quality.

Harvard Business School
September 13th, 2023

Completed tasks 25.1% faster with 40% higher quality.





Things to keep in mind

It's important to keep the following limitations in mind when using LLMs

- 1. They don't learn from interactions.
- 2. Data quality is crucial, including your prompt.
- 3. They don't actually understand.
- 4. They're constrained by context windows.
- 5. They don't always follow your instructions perfectly (alignment) or consistently.
- 6. They can get things wrong or make things up (hallucinations).
- 7. All is resource intensive, and not always the best tool for the job.





Don't blindly trust responses

USER

Question: Write a sentence with the final word 'fear'. To repeat, the last word in the

(-)

Answer must be 'fear':

Answer: The only thing we have to fear is

ASSISTANT

fear itself.

In this example you can see the AI response ignores the direct instruction (alignment), and instead answers based on it's Bias, giving you a false answer. This is often called a hallucination because the AI is "making stuff up", while in this example the hallucination is understandable based on the popular saying, in other examples they can make no sense whatsoever.

Prompting Best Practice



Poll Question Two:

What is your biggest challenge when prompting Al tools?



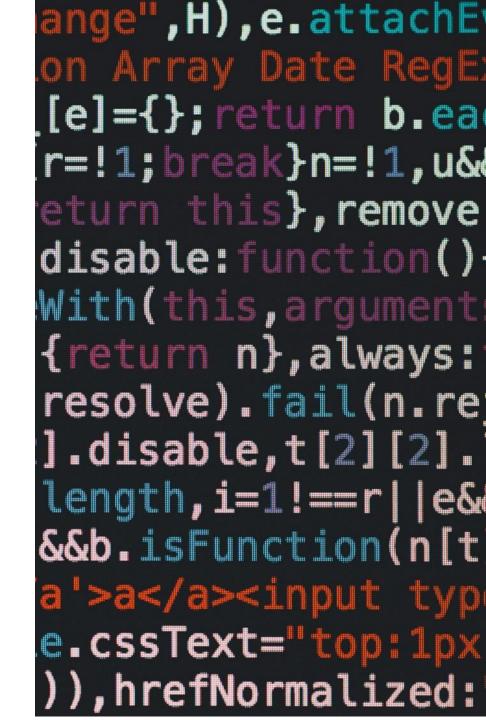
The basics of prompt design

Prompts: To get the best results:

- Be specific
- Add constraints
- Use examples
- Use prompts to create prompts
- Use complete sentences
- Pay attention to grammar, line breaks, capitalization and all that stuff

The CIDI format

- Context: Provide background on the task or goal and the role or personal you want to assign
- Intent: Define what outcome you expect
- Details: Include specifics like target audience, key metrics, or deliverables
- Instructions: Specify output format



Example prompt: Legal Operations

Context Intent Details You are a legal ops lead supporting a global privacy program.

I need you to summarize the key implications of the new EU AI Act

Audience is the IT security team. Use clear, concise language.

Highlight obligations by department.

Return as a bulleted list with section headers.

Instructions

🔐 IT Security & Infrastructure

- Risk Classification Obligations
 - · Classify all AI systems used internally or in products as:
 - Prohibited, High-risk, Limited-risk, or Minimal-risk.
 - Most obligations will apply to high-risk systems (e.g. biometric ID, safety-critical infrastructure, credit scoring tools).
- Security and Resilience Requirements
 - . Ensure robust cybersecurity measures are in place for all high-risk AI systems, including:
 - Protection against data poisoning and model manipulation.
 - · Incident detection and reporting capabilities.
- Logging and Auditability
 - Must enable automatic logging of system decisions and activities to ensure traceability for highrisk Al systems.
- Data Management
 - · Required to ensure training and test data is free of bias, high-quality, and representative.
 - Systems must avoid discriminatory or unauthorized profiling based on sensitive data.

Compliance & Risk Management

- · High-Risk System Obligations
 - Maintain a risk management system across the Al system's lifecycle.
 - Conduct conformity assessments before deploying high-risk AI, and reassess regularly.
- Registration and Transparency
 - · All high-risk systems must be registered in an EU public database.
 - Provide clear user instructions, system capabilities, and limitations.
- Incident Response
 - Must establish protocols for reporting serious incidents or system failures to regulators within 15 days.

Al & Engineering / Developers

- Human Oversight Requirements
 - High-risk systems must be designed to allow human override or intervention.
 - Document who is responsible for monitoring and how oversight is enforced.
- Explainability and Documentation
 - Maintain technical documentation detailing model architecture, training methods, data sets, and performance metrics.
 - Users should be able to understand how decisions are made by the system (especially important for developers building or integrating AI).





Situation: Your healthcare group is releasing a compliance tracking platform to manage staff certifications, required training and audit readiness for HIPAA and state-level healthcare regulations

What risks should we list for our compliance platform?

When listing risks for a compliance platform, it's essential to consider a broad range of potential issues that could impact the platform's effectiveness, the organization's compliance posture, and its overall operations. Here's a comprehensive list, categorized for clarity:

I. Data and Security Risks:

- Data Breach/Unauthorized Access: The risk of sensitive compliance data (e.g., internal audit findings, regulatory filings, personal data) being accessed, stolen, or exposed due to cyberattacks, internal threats, or system vulnerabilities.
- Data Integrity and Accuracy: Risk that the data within the platform is inaccurate, incomplete, or corrupted, leading to incorrect compliance assessments, reports, and decisions. This could stem from manual entry errors, integration issues, or system bugs.
- Data Privacy Violations: Failure to adequately protect personal or sensitive data in accordance with regulations like GDPR, CCPA, HIPAA, etc., within the platform.
- Improper Data Storage: Storing sensitive compliance data in unencrypted or insecure formats, increasing vulnerability.
- Lack of Audit Trails: Insufficient logging of data access, modifications, and system activities, making it difficult to investigate incidents or demonstrate compliance.
- System Vulnerabilities (Software/Hardware): Flaws or weaknesses in the platform's code, infrastructure, or third-party components that could be exploited by attackers.

Outdated Systems and Software: Failure to regularly patch and update the platform and underlying infrastructure, leaving it exposed to known vulnerabilities.

II. Regulatory and Legal Risks:

- Regulatory Non-Compliance: The platform failing to adequately track, interpret, or enforce
 compliance with relevant laws, regulations, industry standards (e.g., PCI-DSS, SOX, HIPAA),
 leading to fines, penalties, and legal action.
- Changing Regulatory Landscape: The risk that new or updated regulations are not promptly
 incorporated into the platform's rules and controls, leading to a gap in compliance.
- Misinterpretation of Regulations: Incorrectly interpreting regulatory requirements when configuring the platform, leading to insufficient or misdirected compliance efforts.
- Legal Action/Lawsuits: Direct legal consequences stemming from compliance failures facilitated or not prevented by the platform.

III. Operational and Systemic Risks:

- Human Error: Mistakes made by users, administrators, or developers of the platform that lead to compliance failures, data issues, or system malfunctions. This includes misconfigurations, incorrect data entry, or neglecting alerts.
- Lack of Monitoring and Alerts: Insufficient real-time monitoring of compliance activities and inadequate alerting mechanisms, preventing timely detection and response to issues.
- System Downtime/Availability: The platform becoming unavailable due to technical failures, cyberattacks, or maintenance issues, disrupting compliance operations.
- Integration Challenges: Difficulties in integrating the compliance platform with other critical systems (e.g., HR, finance, IT security), leading to data silos, inconsistencies, or incomplete compliance visibility.
- · Scalability Issues: The platform's inability to handle increasing data volumes, user numbers,



Situation: Your healthcare group is releasing a compliance tracking platform to manage staff certifications, required training and audit readiness for HIPAA and state-level healthcare regulations

Context

You are a corporate attorney supporting the launch of a Intent healthcare compliance SaaS. Identify overlooked or emerging legal and regulatory risks. Focus on HIPAA, third-party vendors, data use, and operational liabilities. Instructions Prioritize relevance and practical impact. List the top 5 risk areas in bullet points, with 1 short sentence each explaining why they matter.

As a corporate attorney supporting the launch of a healthcare compliance SaaS, here are the top 5 overlooked or emerging legal and regulatory risks, prioritized for relevance and practical impact:

- Fourth-Party Vendor Risk and Sub-Processor Blind Spots: Even with robust third-party
 vendor management, a lack of visibility into your vendors' sub-processors (fourth parties)
 can introduce unmitigated risks to Protected Health Information (PHI) and lead to compliance
 failures, as HIPAA extends liability down the chain.
- AI-Powered Features and Algorithmic Bias/Accuracy: Integrating AI for compliance
 monitoring or data analysis can lead to legal exposure if the algorithms exhibit bias, produce
 inaccurate results, or make discriminatory decisions, potentially violating civil rights laws or
 leading to incorrect compliance assessments.
- Evolving Interoperability Regulations and Information Blocking: New regulations like those stemming from the 21st Century Cures Act are increasing requirements for data exchange, and your SaaS must actively facilitate interoperability and avoid "information blocking" to prevent significant penalties.
- "Shadow SaaS" and Unmanaged Application Use: Employees adopting and utilizing
 unapproved or unmanaged SaaS applications for handling PHI outside of your sanctioned
 platform creates significant security blind spots and compliance gaps under HIPAA's asset
 inventory and access control requirements.
- State-Specific Data Privacy Laws Beyond HIPAA: While HIPAA is central, the increasing
 proliferation of state-specific data privacy laws (e.g., California's CCPA/CPRA, Virginia's
 CDPA) introduces additional and sometimes more stringent requirements for data collection,
 use, retention, and individual rights, which may extend beyond PHI.



Your prompt design checklist

Is your prompt:		An excellent prompt	X A bad prompt
\bigcirc	Clear	Clearly states what you want	Not clear or doesn't give specifics
\bigcirc	Specific	Gives clear instructions	Not very detailed, no specific instructions
\bigcirc	Context Rich	Provides background for the task	Doesn't give enough information
\bigcirc	Readable	Uses simple and concise language	Uses confusing or complicated words
\bigcirc	Constrained	Outlines what you don't want	Has no restraints
\bigcirc	Error-free	No spelling or grammar mistakes	Has grammar or spelling mistakes
0	Well Formatted	Follows correct format and structure	Not organized well

Tips for Better Results

Have a conversation with your Al!

- Al is too vague? Add more context
- Too wordy? Ask for bullets or a summary
- Wrong tone? Provide a tone reference
- Doesn't get it? Break the task into parts
- You just aren't sure? Ask AI to help write or improve your prompt

Remember

 Al gives you a strong starting point — not the final work product. Always review for tone, nuance, and accuracy in your context.



Advanced Prompting Techniques

- Iteration: Taking the LLMs initial response, refining the prompt with additional details or corrections, and asking the AI to generate again. This process can be repeated several times until the desired output quality is achieved.
- 2. Socratic question: Uses a series of probing questions to the LLM to encourage deeper exploration of topics and to produce more nuanced outputs.
- 3. Few shot/many shot: In few-shot learning, a small number of examples are used, while many-shot learning involves several examples. The caution here is that examples can both bias the LLM and limit its responses.
- 4. Self-reflection: ask the AI to critique its output, review its performance, or consider how it might improve. It can be used to get the AI to analyze its responses and reflect on its decisions.

You can use any combination of these techniques; experimenting is essential to improving the responses you get from LLMs.



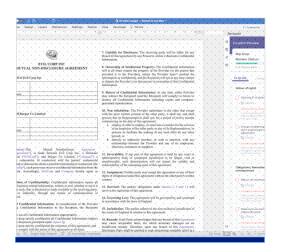


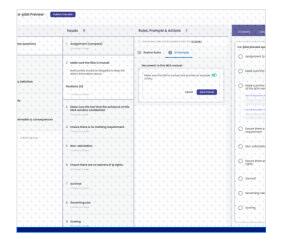
Practical Use Cases



Ways to use Prompts in Contracting

Pre Signature







Post Signature



CONTRACT REVIEW &

Are we indemnified for IP breach in this agreement?

Explain an indemnity vs a liability to a non-lawyer

Rewrite this term to be less restrictive

What else haven't I thought of?

Proof read & check defined terms

PLAYBOOK MANAGEMENT

Tell the AI to review contracts against your standards and what action to take in different scenarios – redline, alert, escalate, comment, use fall back language etc

AUDIT

Do any of our SaaS contracts restrict data storage to US only?

We had a breach or trigger event. Whoa do we need to notify and by when?

Which of my agreements do not cover data privacy obligations?

MIGRATION & Reporting

Extract all obligations for the vendor

Tag parties, terms, renewals, key provisions

Contract Chat

Reviewing an NDA

- Prompt
 Rewrite the Confidentiality Clause.
- Result
 The proposed change isn't what I want.
- Why
 I was not clear in my prompt.

Prompt

Rewrite the confidentality clause

Chat Response

Ok, I am going to REPLACE Rewrite the confidentiality clause

Rewrite the confidentiality clause

Text to delete:

Notwithstanding the above, the Parties agree that information shall not be deemed Confidential Information and the Recipient shall have no obligation to hold in confidence such information, where such information: Is already known to the Recipient, having been disclosed to the Recipient by a third party without such third party having an obligation of confidentiality to the disclosing Party; or Is or becomes publicly known through no wrongful act of the Recipient, its employees, officers, directors, or agents; or Is independently developed by the Recipient without reference to any Confidential Information disclosed hereunder; or Is approved for release (and only to the extent so approved) by the disclosing Party; or Is disclosed pursuant to the lawful requirement of a court or governmental agency or where required by operation of law (such as the California Public Records Act).

Replaced by:

Notwithstanding the foregoing, Confidential Information does not include information that: a.





Reviewing an NDA

- Improved Prompt
 We do not allow marking requirements in an NDA. If this agreement has a marking requirement, please remove it.
- Result
 All found the marking requirement in the agreement, and has proposed the correct revision to remove this from the agreement.
- Why
 I gave relevant information and clear instruction.

Prompt

We do not allow marking requirements in an NDA. If this agreement has a marking requrement, please remove it.

Chat Response

Ok, I am going to REPLACE Remove marking requirement for Confidential Information

Remove marking requirement for Confidential Information

Text to delete:

Either Party may disclose Confidential Information to the other Party in confidence provided that the disclosing Party identifies such information as proprietary and confidential either by marking it, in the case of written materials, or, in the case of information that is disclosed orally or written materials that are not marked, by notifying the other Party of the proprietary and confidential nature of the information, such notification to be done orally, by e-mail or written correspondence, or via other means of communication as might be appropriate.

Replaced by:

Either Party may disclose Confidential Information to the other Party in confidence provided that the disclosing Party identifies such information as proprietary and confidential by notifying the other Party of the proprietary and confidential nature of the information, such notification to be done orally, by e-mail or written correspondence, or via other means of communication as might be appropriate.

Contract Chat

Reviewing an NDA

- Prompt
 - Does this agreement have an indemnity clause?
- Result
 - Answered the question and provided the relevant information.
- Why
 - Gives you the ability to fact check and confirm the Al answer.

Prompt

Does this agreement have an indemnity clause?

Chat Response

Yes, the agreement contains an indemnity clause. The relevant text from the contract is as follows:

 The Recipient will indemnify the disclosing Party, the disclosing Party's Representatives and any Related Party of the disclosing Party against any losses, damages, costs, claims, expenses, liabilities, proceedings or demands which the disclosing Party, its Representatives or its Related Parties may incur or suffer as a result of a breach of this agreement by the Recipient or its Representatives [1].

Contract Reference

7. The Recipient will indemnify the disclosing Party, the disclosing Party's Representatives and any Related Party of the disclosing Party against any losses, damages, costs, claims, expenses, liabilities, proceedings or demands which the disclosing Party, its Representatives or its Related Parties may incur or suffer as a result of a breach of this agreement by the Recipient or its Representatives.

Spend Management



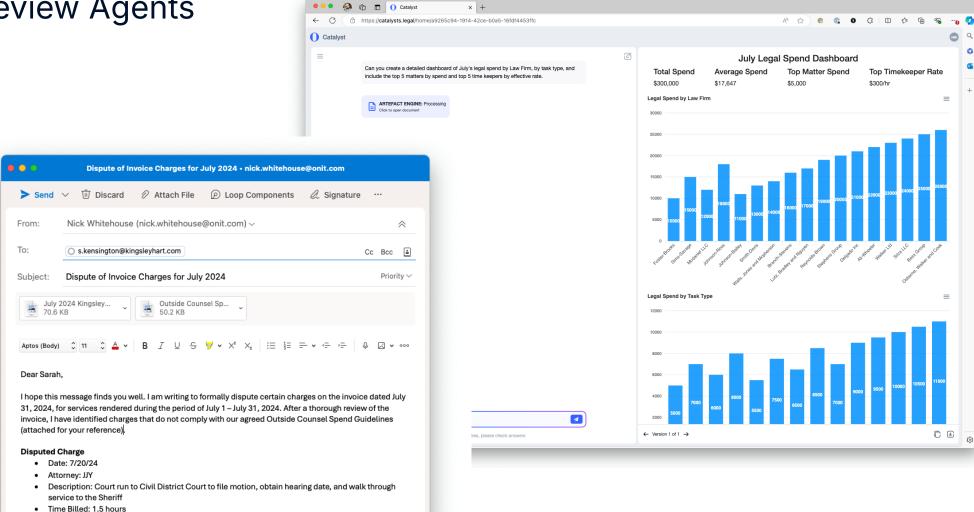
Invoice Review Agents

Rate: \$475/hourTotal Amount: \$712.50

Reason for Dispute

UTBMS Code: A101 (Filing and Organizing Documents)

According to our Outside Counsel Spend Guidelines, administrative tasks such as filing, organizing



Draft saved just now



🎢 Legal Spend Chat

Reviewing Legal Spend

Prompt

Can you create a detailed dashboard of July's legal spend by Law Firm, by task type and include the top 5 matters by spend and top 5 timekeepers by effective rate.

Result

Dashboard with charts showing requested information.

Now What?

Ask follow-up questions for additional insight.

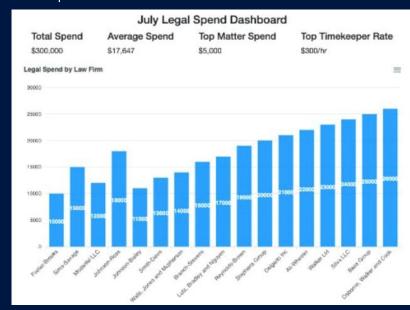
- Compare this to my legal spend for July 2024
- o Who are my top timekeepers by spend?
- What has been the trend of my legal spend over the last 6 months?
 Show this in a line graph

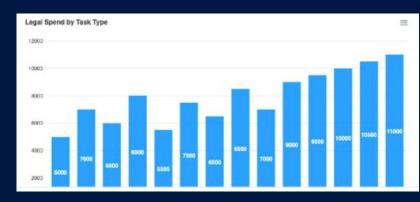
Onit

Prompt

Can you create a detailed dashboard of July's legal spend by Law Firm, by task type, and include the top 5 matters by spend and top 5 time keepers by effective rate.

Chat Response





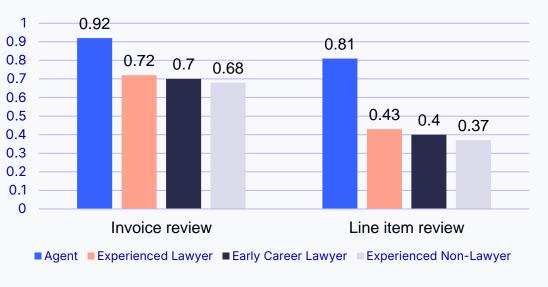
Agent performance

Onit has been experimenting with a range of Legal Al Agents that perform at and above experienced legal professionals on legal specific tasks.

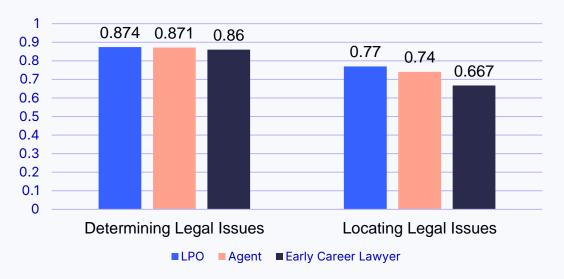
We've run extensive industry wide research to test these Agents:

- In spend management, the Agent was 20% more accurate at invoice review than the best performing human reviewers.
- 38% more accurate at line-item review than the <u>best</u> <u>performing</u> human reviewers.
- And 22x faster than the <u>fastest</u> human reviewers.
- In contract review, the Agent was as accurate as outsourced legal providers.
- And 76x faster than the <u>fastest</u> human reviewers.

Spend Agent Performance



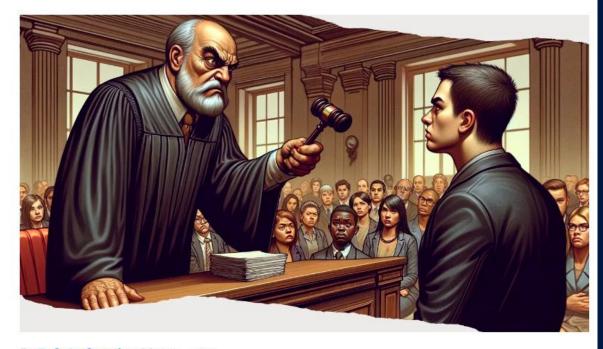
Contract Agent Performance







Al Hallucinations Strike Again: Two More Cases Where Lawyers Face Judicial Wrath for Fake Citations



By Bob Ambrogi on May 14, 2025



In what has become a distressingly familiar pattern in courtrooms across America, two more cases have emerged of lawyers submitting briefs containing non-existent legal citations generated by AI tools.



Large language models (LLMs) generate text by identifying patterns in vast datasets, but they lack true legal understanding and are not connected to verified legal databases. This limitation can result in confidently stated but fabricated case law—a phenomenon known as "hallucination."

In 2025, attorneys from Ellis George and K&L Gates were sanctioned after submitting a brief with fake Al-generated citations—nine of 27 were inaccurate, including two fictional cases. The court struck the filings, imposed \$31,000 in sanctions, and called their reliance on unchecked Al "scary."

You should ALWAYS ask if the source is verifiable and understand the risks of relying on unvalidated legal content.



How can these systems be misused?

The Center for Al Safety lists four categories of risk of this new Al

Malicious use

- Cyberterrorism
- Bioterrorism
- Persuasive AI (disinformation)
- Concentration of power

• The AI race / competition

- Military Al arms race
- Corporate Al arms race
- Evolutionary dynamics

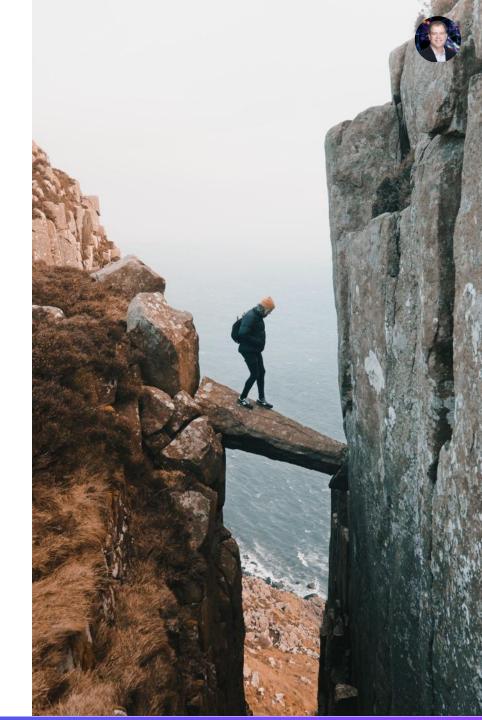
Organizations

Exponential accidents

Rogue Als

- Proxy gaming
- Goal drift
- Power seeking
- Deception





At Onit we follow a research-based approach to develop transparent, explainable and legally relevant Al solutions that are:

- 1. Explainable
- 2. Contestable
- 3. Beneficial
- 4. Human-centered
- 5. Reliable
- 6. Secure



