



# Scaling AI, responsibly

## Tools & Technology deep dive

**Nemko Digital**

September 11, 2025

# With you today

## Bas Overtoom

*Senior AI Trust Expert*



- **Experienced AI & Data Executive**

Over a decade of consultancy experience, driving AI and data transformations for top global organizations.

- **Responsible AI Advocate**

Passionate about responsible AI to address business, social, and environmental challenges.

- **Global Business Expertise**

Strong international background, including seven years in Asia, fostering cross-cultural collaboration. Leads global business development at Nemko Digital, promoting AI Trust worldwide.

- **VC Advisor for AI Scale-Ups**

Supports AI startups within a prominent Dutch VC fund to achieve global growth.

## Pepijn (Pep) van der Laan

*Global Technical Director*



- **Scaling AI Impact**

Over a decade of experience in realizing business value through scaling AI and ML from initial proof-of-concept to enterprise-wide solutions.

- **AI Strategy Advisory**

Extensive experience shaping the AI transformation for global leaders and national champions across industries.

- **AI Capability building**

Led a team of 90 data scientists through the transformation from the traditional consulting model and introducing modern delivery and development practices.

- **Growing AI Trust**

Recognized for consistently bridging the gap between the developer and AI risk communities, building mutual understanding



# Nemko Digital: Compliance without Complexity

## Nemko Digital is part of Nemko Group

We empower our customers through innovative digital solutions and expert guidance.

We aim to build digital trust and help navigate the complexities of the modern online landscape, with a special focus on Artificial Intelligence.

We combine an in-depth knowledge of regulation and market-leading frameworks with an entrepreneurial stance and a maker's mindset.



AI GOVERNANCE

AI COMPLIANCE

AI MATURITY

AI ASSURANCE



NIST



Maturity Model



Trust Mark



# At Nemko Digital we believe that AI Trust is a growth enabler



*Compliance with upcoming regulation*



*Reputation as leading global company*



*Control to prevent incidents / harm*



*Stakeholder demands around use of AI*



*Competitive advantage in the market*



# What is top-of-mind for our clients?

We deliver Digital Trust through end-to-end compliance and advisory support, combining technical, regulatory, and process expertise.



## How to get ready for the EU AI Act?

- Risk categorization of AI systems
- Achieving and demonstrating conformity
- Ensuring market access for products



## How to assure AI algorithms technically?

- Design validation and robustness testing
- Bias detection and mitigation
- Ongoing algorithmic assurance processes



## How to get ISO certified for AI, Data, and Security?

- Organizational readiness and training
- Management System implementation
- Audit and certification



## How to monitor and govern AI & Data at scale?

- Performance metrics and benchmarking
- AI governance tooling and automation
- Scalable monitoring frameworks



## How to ensure market access for AI products?

- Applicability of various directives and regulations
- Roadmap towards compliance for Digital Trust
- Achieving and demonstrating conformity



## How to structure an AI & Data operating model?

- Defining roles and responsibilities
- Establishing controls, processes, and oversight
- Integrating governance into business workflows



## How to instill trust in AI-embedded products?

- Nemko's Trust Mark as a standard
- Proactively achieving a statement of conformity
- Pre-empting client's procurement questions



## How to align AI & Data strategy and maturity?

- Linking value realisation with AI adoption
- Setting risk appetite and ethics principles
- Building AI & Data literacy across the organisation



# Today we will talk about scaling



## How to get ready for the EU AI Act?

- Risk categorization of AI systems
- Achieving and demonstrating conformity
- Ensuring market access for products



## How to get ISO certified for AI, Data, and Security?

- Organizational readiness and training
- Management System implementation
- Audit and certification



## How to ensure market access for AI products?

- Applicability of various directives and regulations
- Roadmap towards compliance for Digital Trust
- Achieving and demonstrating conformity



## How to instill trust in AI-embedded products?

- Nemko's Trust Mark as a standard
- Proactively achieving a statement of conformity
- Pre-empting client's procurement questions



## How to assure AI algorithms technically?

- Design validation and robustness testing
- Bias detection and mitigation
- Ongoing algorithmic assurance processes



## How to monitor and govern AI & Data at scale?

- Performance metrics and benchmarking
- AI governance tooling and automation
- Scalable monitoring frameworks



## How to structure an AI & Data operating model?

- Defining roles and responsibilities
- Establishing controls, processes, and oversight
- Integrating governance into business workflows



## How to align AI & Data strategy and maturity?

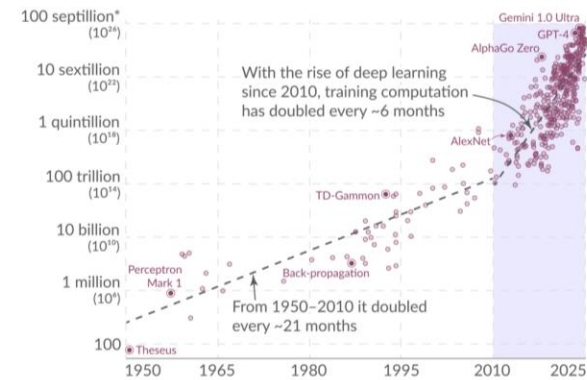
- Linking value realisation with AI adoption
- Setting risk appetite and ethics principles
- Building AI & Data literacy across the organisation



# The many moving parts make scaling AI difficult

## Speed of innovation

Training FLOPs of AI systems



## Evolving regulation

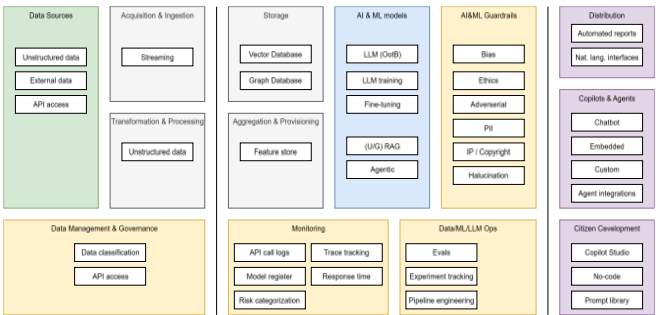
EU Acts and Directives related to AI, Data, and Cyber

| Domain                                | EU Regulation                                 | Applicability  |
|---------------------------------------|-----------------------------------------------|----------------|
| Artificial Intelligence               | AI Act                                        | Adopted / 2026 |
|                                       | General Data Protection Regulation (GDPR)     | In force       |
|                                       | Data Act                                      | In force       |
|                                       | Data Governance Act                           | In force       |
| Data protection and governance        | ePrivacy regulation                           | In draft / TBC |
|                                       | Cyber Resilience Act (CRA)                    | In force       |
|                                       | Network Information Security Directive (NIS2) | Adopted / 2027 |
|                                       | Digital Operational Resilience Act (DORA)     | In force       |
| Cyber security and digital resilience | Cybersecurity Act                             | In force       |
|                                       | Product Liability Directive - revised         | Adopted / 2026 |
|                                       | Radio Equipment Directive (RED)               | In force       |
|                                       | Machinery Regulation - revised                | Adopted / 2027 |
| Product Safety and Conformity         | General Product Safety Regulation (GPSR)      | In force       |
|                                       | Digital Services Act (DSA)                    | In force       |
|                                       | Digital Markets Act (DMA)                     | In force       |
|                                       | European Health Data Space (EHDS)             | Adopted / 2026 |
| Market and Critical Infrastructure    |                                               |                |
| Sector-specific                       |                                               |                |



## New architecture requirements

New/enhanced capabilities due to GenAI



## AI in everything



## Multiple standards



## Human nature



# What keeps executives up at night

Common pain points

How do I **convince** my CRO that we have all AI risks under control?

How do I manage compliance when I have **100s of AI-products**?

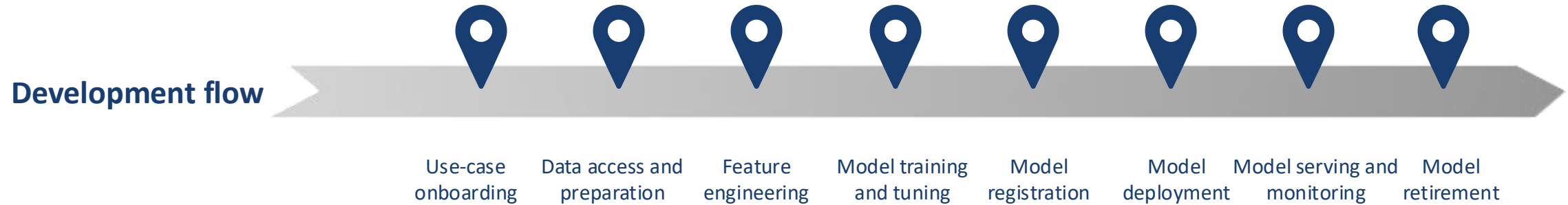
How do we ensure that our AI-products don't **fail silently**?

How can we stay in control over products with **Agentic AI**?

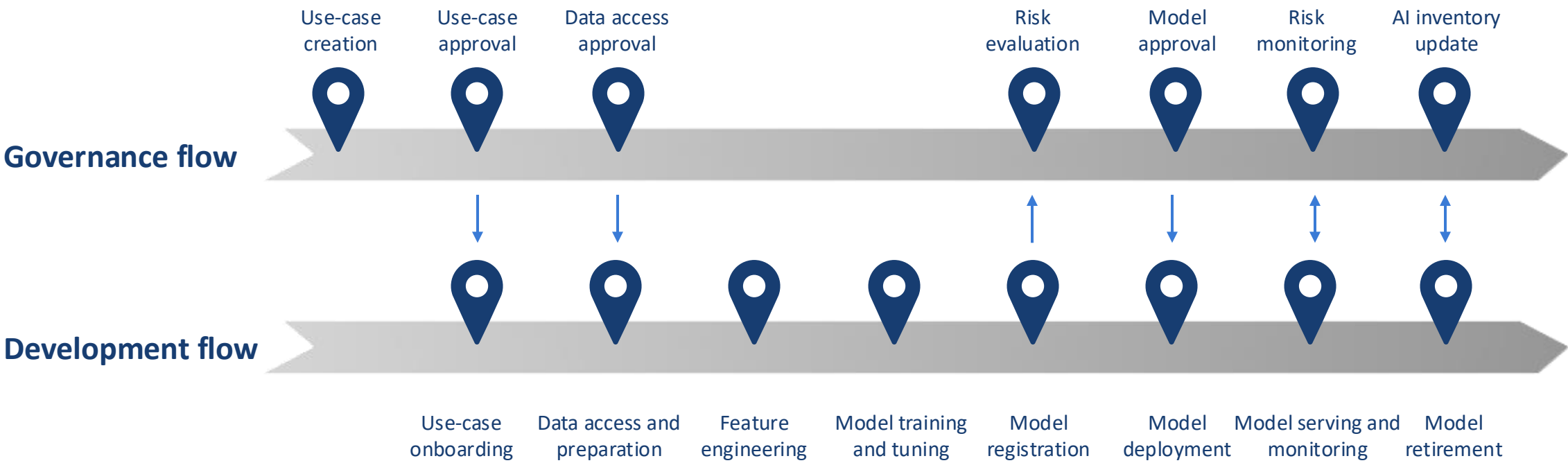
How do I ensure that our AI-products **remain reliable** in a changing environment?



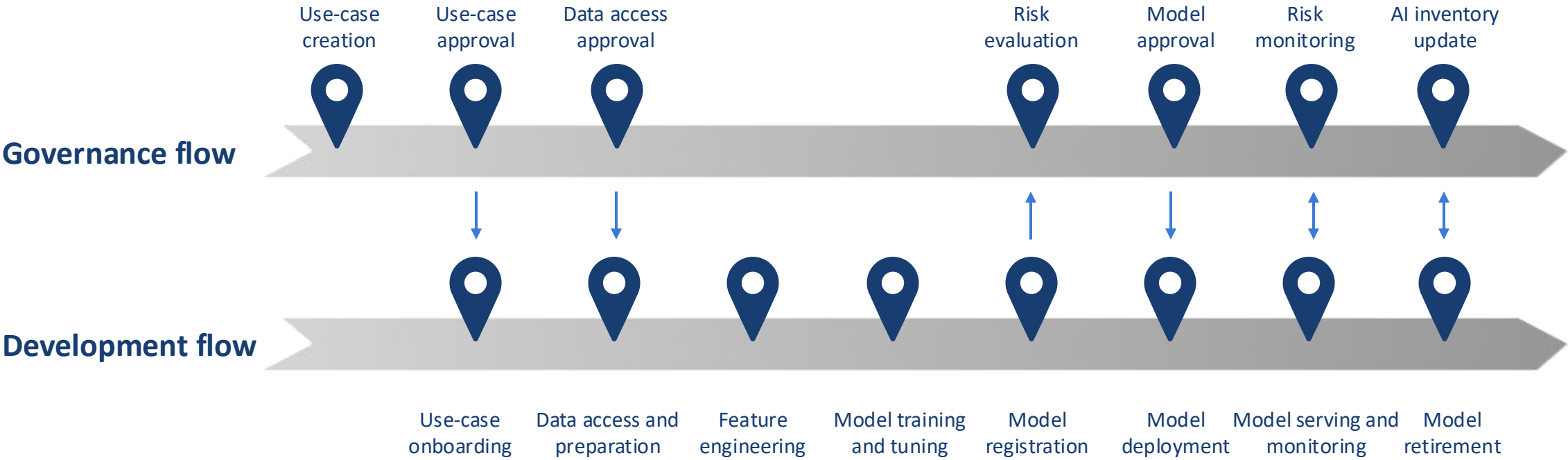
# The right tooling enables the scaling of AI maturity



# The right tooling enables the scaling of AI maturity



# The right tooling enables the scaling of AI maturity



Direct benefits of Tooling  
for Management and Governance

Life Cycle  
Management

Risk  
Management

Compliance  
Management



# Key features of solid AI governance solutions



## Life Cycle Management

- **AI Inventory Management**  
Centralized repository for all AI models, enhancing transparency and tracking across the organization.
- **Model Performance Monitoring**  
Real-time AIOps for performance tracking, data drift detection, and anomaly identification.
- **Bias Detection and Mitigation**  
Advanced tools to assess and correct biases within AI models to support fairness and ethical AI usage.



## Risk Management

- **Risk Tracking and Mitigation**  
Frameworks for assessing and mitigating AI-related risks, ensuring accuracy, resilience and reliability.
- **Risk Visibility and Control**  
Insight in vulnerabilities and risk patterns across your AI inventory, based on prioritized metrics and controls.
- **Streamlined Governance**  
Set policies, define roles, processes, and approval flows to ensure compliance and accountability.



## Compliance Management

- **Regulatory Completeness**  
Access to global AI regulatory databases to track evolving legal and ethical requirements.
- **Automated Compliance Reporting**  
Streamlined regulatory compliance processes with automated documentation and audit trails.
- **Audit and Explainability Tools**  
Mechanisms for AI transparency, enabling explainable AI and clear documentation of decision-making processes.



# Mapping the tool landscape (simplified)

| Archetypes                     | Typical market positioning                                                                                                                                    | Players (indicative)                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Hyperscalers</b>            | <ul style="list-style-type: none"> <li>One-stop-shop for broad range of services</li> <li>Fast-follower / last mover strategy</li> </ul>                      |                                                                                                                                                                            |
| <b>Integrated AI platforms</b> | <ul style="list-style-type: none"> <li>Opiniated (often lakehouse-type) architecture</li> <li>Balancing governance and developer experience</li> </ul>        |      |
| <b>MLOps tools</b>             | <ul style="list-style-type: none"> <li>Initially developed for science and ML workflows</li> <li>Evolving to address (Gen)AI requirements</li> </ul>          |                                                                                         |
| <b>LLMOps tools</b>            | <ul style="list-style-type: none"> <li>Designed to cater to the specific needs of GenAI</li> <li>Emphasis on developer experience and cost control</li> </ul> |                                                                                       |
| <b>Governance tools</b>        | <ul style="list-style-type: none"> <li>Focus on AI inventory and policy management</li> <li>Prone to tie-in professional services with offering</li> </ul>    |                                                                                 |



# Our selection framework for AI Governance Tools



## Market presence

- Track record of proven success
- Reliability and durability of solution
- Availability of skills in the talent market



## Tool capabilities

- Fit with functional and requirements
- Quality standards
- Ease of configuration



## Innovation

- Product vision, strategy, and roadmap
- Supplier's innovation capabilities and track record
- Opportunities for co-development



## Support

- SLA commitments
- Service delivery track-record
- Onboarding and training resources



## Integration

- System resource requirements
- Compatibility with existing landscape
- Available connectors (ingress and egress)



## Compliance

- Cyber security and risk management standards
- Regulatory compliance
- Data sovereignty



## TCO

- CapEx and OpEx costs (license, maintenance, etc.)
- Features v. Time v. Cost trade-off
- Supplier lock-in



# Our selection framework for AI Governance Tools



## Market presence

- Track record of proven success
- Reliability and durability of solution
- Availability of skills in the talent market

Does supplier have **sufficient backing**?



## Tool capabilities

- Fit with functional and requirements
- Quality standards
- Ease of configuration

Is this really **your archetype**?



## Innovation

- Product vision, strategy, and roadmap
- Supplier's innovation capabilities and track record
- Opportunities for co-development

Is the **vision** aligned with your needs?



## Support

- SLA commitments
- Service delivery track-record
- Onboarding and training resources

Where will we need **internal capabilities**?



## Integration

- System resource requirements
- Compatibility with existing landscape
- Available connectors (ingress and egress)

Will this really work with **your stack**?



## Compliance

- Cyber security and risk management standards
- Regulatory compliance
- Data sovereignty

Does the tool cater to **local** and **industry** needs?



## TCO

- CapEx and OpEx costs (license, maintenance, etc.)
- Features v. Time v. Cost trade-off
- Supplier lock-in



# Quiz



# IBM's watsonx.governance



## Backing

- IBM is a global IT solutions powerhouse
- Analyst accolades from a.o. Forrester and IDC
- Implemented a.o. at IBM itself (>5,500 objects under governance)



## Integration

- Part of watsonx AI & Data platform
- Offered as independent solution
- Integrates with 3<sup>rd</sup> party solutions including AWS and MS and others
- Allows for cloud and on-premise deployment



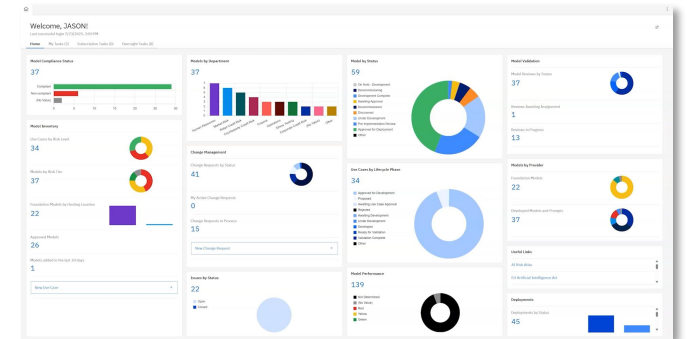
## Product vision

Direct, manage and monitor your AI using a single toolkit to speed up responsible, transparent, explainable AI

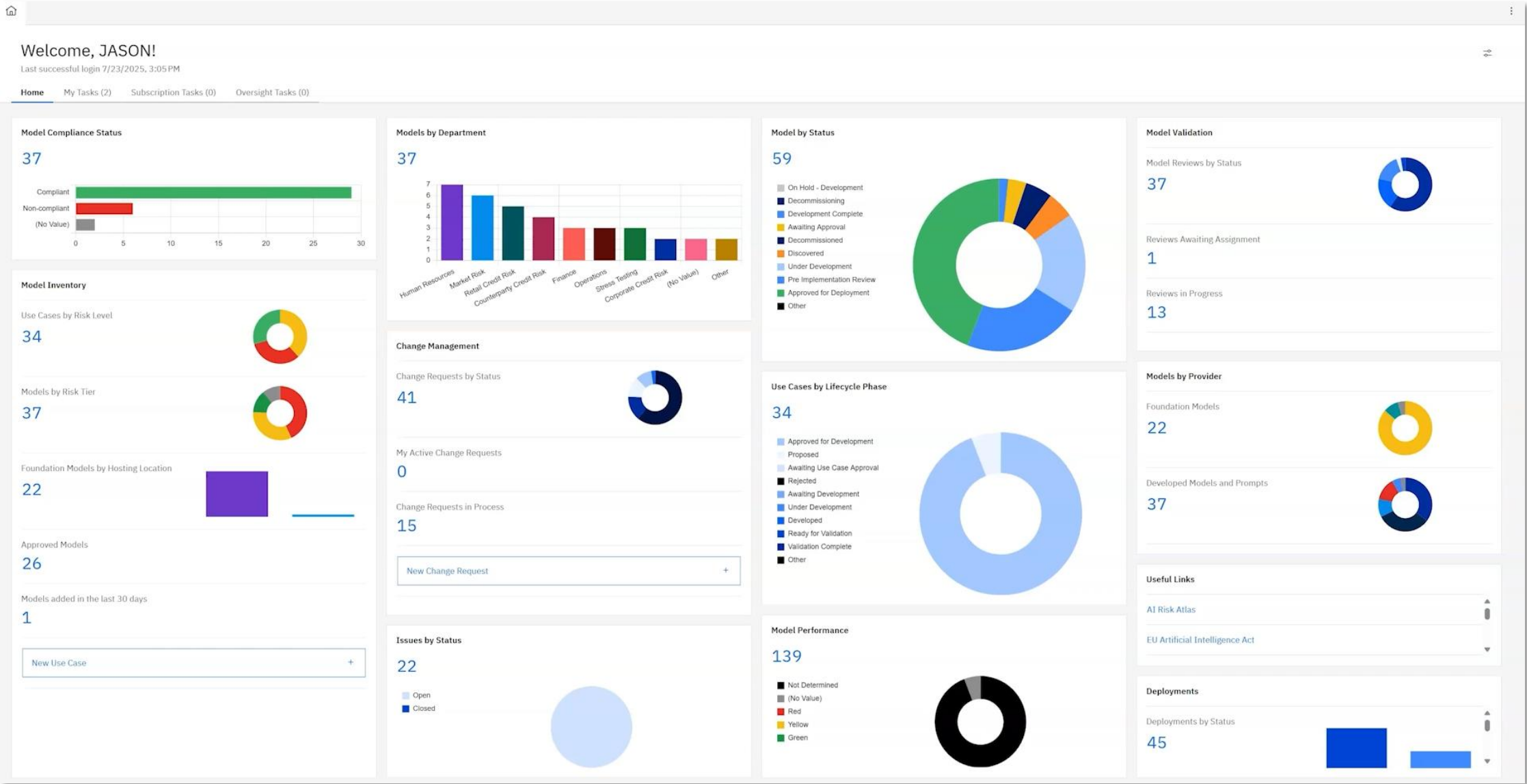


## Key features

- AI inventory
- Risk categorization
- Compliance management
- Policy management
- Lifecycle management
- Automated workflows



# watsonx.governance dashboard



# watsonx.governance model fact sheets

Projects / gov-demo / Finance news summarization - Z...

Open in Prompt Lab

AI Factsheet

Evaluate

Governance

Foundation model

Prompt template

Prompt parameters

Evaluation

Attachments

Other attachments

task type

Summarization

Created by PAUL Hake

Date

Prompt

Variables {Input}

Prompt p

Decoding

Finance news summarization - zero shot - v0

Track in AI use case

Govern prompt template through the AI lifecycle, from request to productive use.

Define AI use case

Define approach

Assign model versions

Define approach

Use case: Finance News A

An approach defines one p

Each approach can include

New approach +

Extraction w Llam

Evaluation activity

Last evaluation activity

November 09, 2023 at 10:19:46 AM

Evaluation data set

SentimentTestDataValidation.csv

Threshold alerts

1

Quality

Accuracy

0.846

Weighted False Positive Rate (wFPR)

0.096

Weighted precision

0.890

Weighted True Positive Rate (wTPR)

0.846

Weighted recall

0.846

Weighted F1-Measure

0.848



# Deeploy



## Backing

- Dutch startup, founded in 2020
- € 6.4M in seed and series A
- € 7.5M grant from the European Innovation Council in 2025
- Main clients in Finance and Health industries



## Integrations

- Platform comes as SaaS or Private Cloud
- On AWS and Azure marketplaces
- Integrates with a.o. Databricks
- UI interface and python client for data scientists



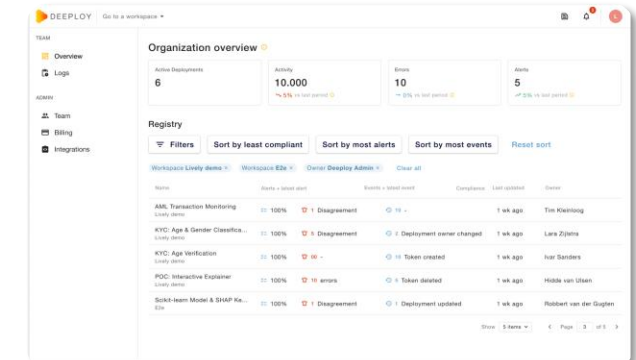
## Product vision

Responsibly deploy any ML or AI model; ensuring transparency, compliance and control. Comply with the AI Act.



## Key features

- Deployment and integration
- Performance and drift tracking
- Alerts and model comparison
- Audit trails and model tracking
- Explainability



# Model deployment and monitoring

### Model Details

Repository

Select the repository, branch, and commit used for your Deployment

Repository

Branch

Commit

Use root folder

Model

Configure the model details for your Deployment

Model framework

Serverless

CPU request/limit

Memory request/limit

Model

Model framework

Serverless

CPU request/limit

Memory request/limit

### Deployments

| Model                                                                            | Alerts                             | Compliance                           | Accuracy               |
|----------------------------------------------------------------------------------|------------------------------------|--------------------------------------|------------------------|
| <div><div></div><div>NLP Sentiment Classification</div><div>Standard</div></div> | <div><div></div><div>0</div></div> | <div><div></div><div>80%</div></div> | <div><div></div></div> |
| <div><div></div><div>KNN Income Classifier</div><div>External</div></div>        | <div><div></div><div>3</div></div> | <div><div></div></div>               | <div><div></div></div> |
| <div><div></div><div></div><div>Register</div></div>                             | <div><div></div></div>             | <div><div></div></div>               | <div><div></div></div> |
| <div><div></div><div></div><div>Standard</div></div>                             | <div><div></div><div>0</div></div> | <div><div></div></div>               | <div><div></div></div> |

### Monitoring

Accuracy

65%

Precision

46%

Recall

56%

F1

66%

Recall

1

2

3

4

5

6

7

Repository

Deployment

Model

Explainer

Transformer

Compliance

Deploy

Summary of Deployment

Review the summary below for accuracy and completeness before deploying

Back

Next

Request approval

Repository

Repository

Branch

Commit

Deployment

Deployment backend

Name

Model

Model framework

Serverless

CPU request/limit

Memory request/limit

example-sklearn-census

master

Merge branch 'master' into master

KServe

d

scikit-learn

Yes

0.1/0.1

256/256



# Governance and approval flows

## Documentation & Checklists

EU AI Act High-Risk Requirements Checklist

Fundamental Rights Impact Assessment (FRAIA) Documentation

Data Protection Impact Assessment (DPIA) Checklist

## EU AI Act High-Risk Requirements

- ✓ Events are automatically logged and traceable
- ✗ The linked repository is private
- ✓ Feature value boundaries are documented
- ✗
- ✗

Version 1.42

Deploy

### Approval

Lara Zijlstra ✓  
Robbert van der Gughten !  
The new commit doesn't have metadata

### Events

Date & time range

| Status | Event                          | Executed by       | Timestamp              |
|--------|--------------------------------|-------------------|------------------------|
| ✓      | Token deleted                  | Lara Zijlstra     | 15-04-2024 10:11 GMT+2 |
| ↻      | Deployment description updated | Deeploy Dev Admin | 15-04-2024 10:11 GMT+2 |
| ✗      | Deployment updated             | Markus Heid       | 15-04-2024 10:11 GMT+2 |
| ✓      | Deployment owner changed       | Anouk Wolters     | 15-04-2024 10:11 GMT+2 |
| ✓      | Token created                  | Matilde Alves     | 15-04-2024 10:11 GMT+2 |

## Data Protection Impact Assessment (DPIA)

Export PDF

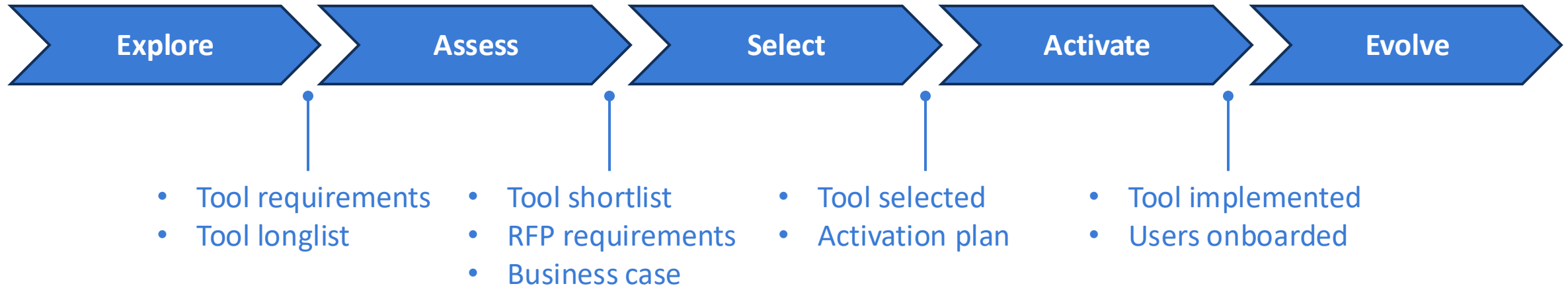
STEP 1: IDENTIFY THE NEED FOR A DPIA

Explain broadly what project aims to achieve and what type of processing it involves.

STEP 2: DESCRIBE THE PROCESSING



# The Next Step: Our approach for selecting the right tooling



**Direct benefits of Tooling  
for AI Management and Governance**



**Life Cycle  
Management**



**Risk  
Management**



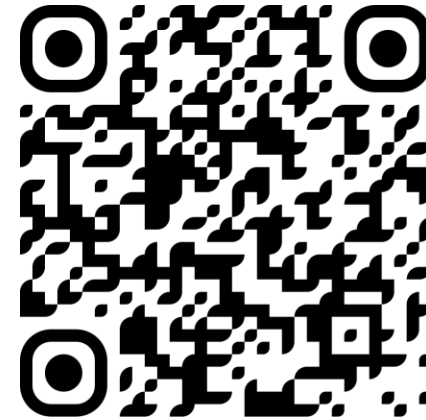
**Compliance  
Management**



## Next steps



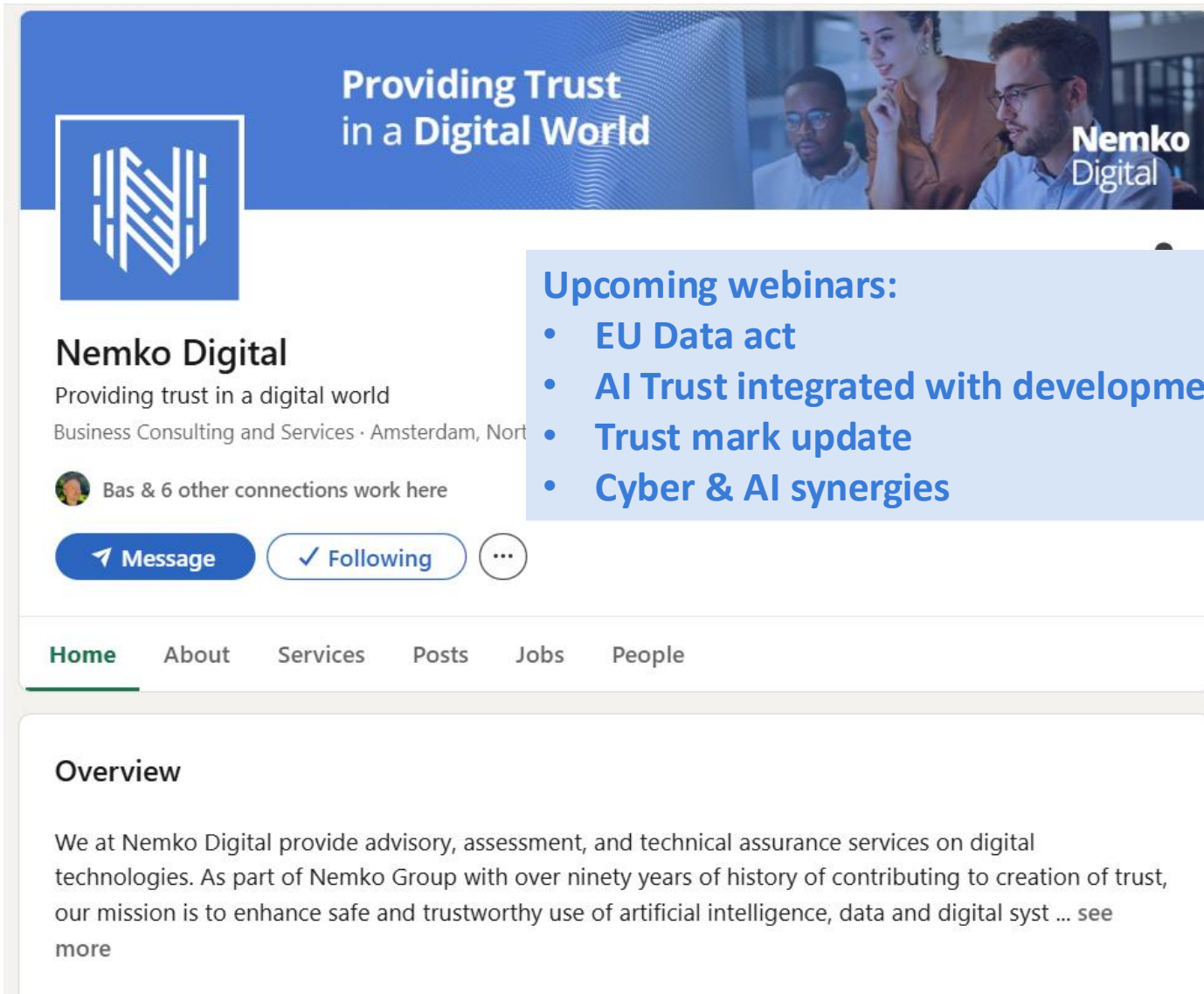
# *AI Tooling Exploration:* Tailored Insights in a 30 mins call



In this session to help evaluate your requirements and how we can best support you and your team.



# Keep track of our upcoming webinars via our LinkedIn community



**Providing Trust in a Digital World**

**Nemko Digital**  
Providing trust in a digital world  
Business Consulting and Services · Amsterdam, North Holland

Bas & 6 other connections work here

Message Following

**Upcoming webinars:**

- EU Data act
- AI Trust integrated with development
- Trust mark update
- Cyber & AI synergies

**Overview**

We at Nemko Digital provide advisory, assessment, and technical assurance services on digital technologies. As part of Nemko Group with over ninety years of history of contributing to creation of trust, our mission is to enhance safe and trustworthy use of artificial intelligence, data and digital syst ... see more

## Follow us!

Join us on LinkedIn or at the AI Hub, where we regularly share insights, videos, news, webinars, and other engaging content.



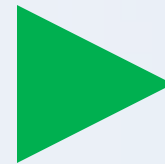
For complete details about our services, visit [digital.nemko.com](https://digital.nemko.com) or explore our brochure.



# AI Trust is about enabling innovation: faster, safer, and at scale



**Stop** bolting on trust as a **feature**



**Start** building with it as the **foundation**





**Nemko**  
Digital