

2024

# Focus on AI in the Dutch central government



Netherlands  
Court of Audit

## **Abbreviations of Dutch ministries**

A&M	Asylum and Migration
AZ	General Affairs
BZ	Foreign Affairs
BZK	Interior and Kingdom Relations
VRO	Housing and Spatial Planning
EZ	Economic Affairs
KGG	Climate Policy and Green Growth
I&W	Infrastructure and Water Management
J&V	Justice and Security
LVVN	Agriculture, Fisheries, Food Security and Nature
OCW	Education, Culture and Science
SZW	Social Affairs and Employment
VWS	Health, Welfare and Sport

# Contents

1. **Executive summary | 4**
  2. **About this investigation | 7**
    - 2.1 Why this investigation? | 7
    - 2.2 Definition of AI | 8
    - 2.3 AI Act | 9
    - 2.4 Audit approach | 10
    - 2.5 Structure of this report | 11
  3. **The use of AI in central government | 12**
    - 3.1 How often is AI deployed? | 12
    - 3.2 AI applications | 16
  4. **Opportunities of AI | 20**
    - 4.1 Opportunities and results | 20
    - 4.2 Obstacles | 22
  5. **AI risks | 25**
    - 5.1 Risk management | 25
    - 5.2 Risk classification | 28
  6. **Response | 33**
- Appendices | 34**
- Appendix 1 Methodology | 34
  - Appendix 2 Selected organisations | 37
  - Appendix 3 Literature | 41
  - Appendix 4 Endnotes | 42

# 1.

# Executive summary

**Artificial intelligence (AI) is being deployed by many government organisations in the Netherlands, although only a limited number of AI systems are being used per organisation. The systems are applied mainly to retrieve and process data in applications that do not directly impact citizens or businesses. AI's greatest potential, according to the organisations, lies in its ability to increase workflow efficiency, for instance by overcoming staff shortages. However, the organisations do not know if their systems are living up to expectations. They have not assessed the opportunities and potential risks of more than half of their AI systems. Where they have, they have used a wide variety of assessment instruments. The government organisations have classified 30 of their AI systems as high risk. They have an incentive to downplay risks: systems that are not high risk do not need to meet the strict requirements of the AI Act.**

The Dutch central government is making more and more use of AI in its operations and performance to improve service delivery and workflow efficiency. But AI is not without risk; it can lead to bias and privacy violation. To function and perform correctly, government organisations must use AI responsibly, maximise the opportunities and mitigate the risks. According to the Netherlands Court of Audit, this is not possible without understanding how AI is used. Parliament cannot oversee the responsible use of AI if it does not know how the government uses it and what the opportunities and risks are. With this investigation, the Court of Audit provides a first insight into the use of AI in central government. Introduction of the AI Act on 1 August 2024 further increased the need for such insight.

This European regulation imposes obligations on the development and use of AI systems. As from February 2025, for instance, the use of certain AI systems by both governmental and non-governmental organisations will be prohibited.

For this investigation, we analysed the AI systems in use now and in the past at 70 government organisations, all of which responded to our requests for information. Most said they were already using AI systems, although they only used a few. Nearly all of them used 3 at most. In total, the organisations named 433 AI systems. At the time of our investigation, 120 systems (28%) were actually in use.

AI is used mainly in applications that do not directly impact citizens or businesses, such as data retrieval and processing applications, or applications to optimise internal processes. Some AI systems, however, do have a direct impact on citizens and businesses, for instance when applied in inspection and enforcement procedures or in service delivery.

Government organisations believe AI's greatest potential lies in improving the efficiency of internal processes, for instance by overcoming staff shortages. However, the organisations do not know whether a third of their systems are living up to expectations. They name several obstacles that prevent them from maximising the potential of AI: lack of expertise and capacity, uncertain data-sharing laws and regulations, unsuitable infrastructure and the ever-heavier compliance burden.

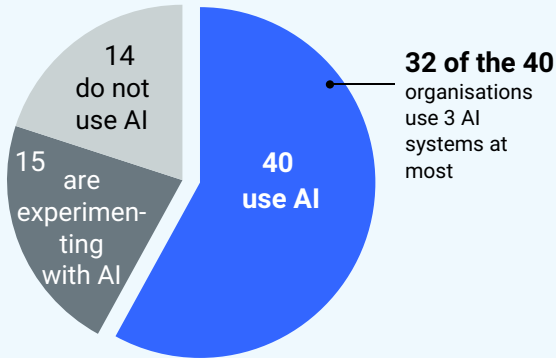
The potential risks of more than half the reported AI systems, including a third of the high-risk systems, have not been assessed. Where they have been, they have not been assessed uniformly. The assessment instruments range from privacy checks and AI assessment frameworks to self-developed risk analyses. There is no government-wide risk assessment instrument.

The organisations classify most of their AI systems as minimal risk, within the meaning of the AI Act. This does not mean they are risk free. There is always the risk of privacy violations. Under the AI Act, minimal or limited-risk systems must comply with applicable laws and regulations, such as the General Data Protection Regulation (GDPR) and, in the Netherlands, the Government Information Security Baseline (BIO). None of the organisations thought their AI systems harboured unacceptable risks, but some were uncertain whether they were using 'prohibited' systems.

# AI in central government

## AI usage at 70 organisations

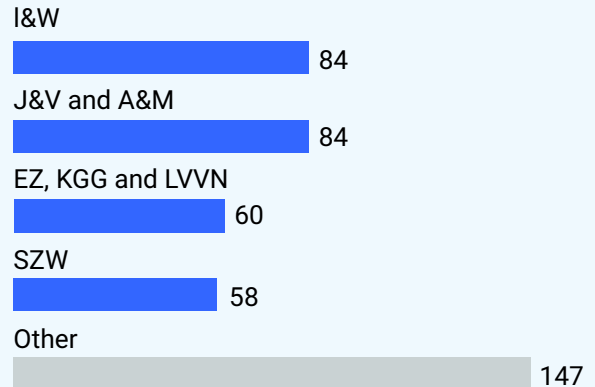
Most organisations use AI\*



\*The total number of organisations adds up to 69 because the Ministry of LVVN and the Ministry of EZ have been combined.

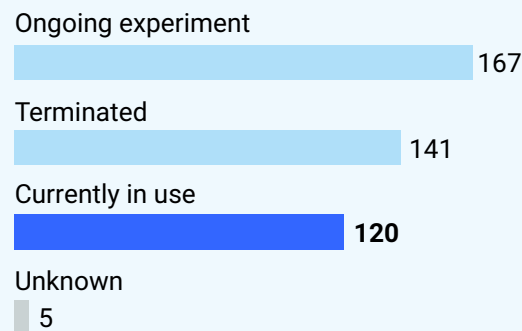
## Ministries with the most AI

I&W, J&V and A&M make most use of AI

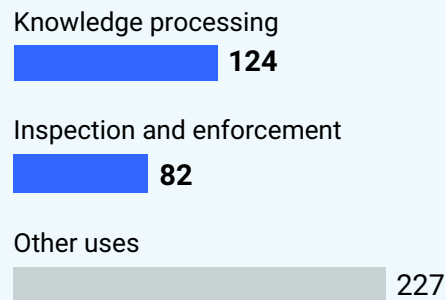


## The 433 AI systems

120 AI systems are currently in use

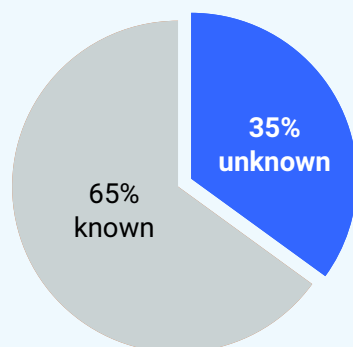


AI mainly used for **Knowledge processing, and inspection and enforcement**



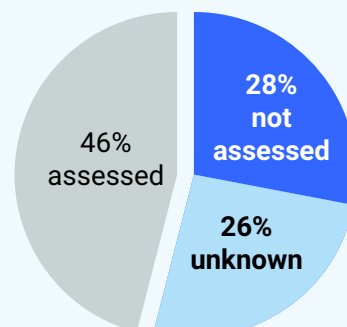
## Results

The results of 35% of the AI systems are **unknown**



## Risk assessment

No demonstrable risk assessment of 54% of the AI systems



# 2.

# About this investigation

## 2.1 Why this investigation?

The Dutch government is making greater use of AI to improve its performance and operation. The Strategic Action Plan for Artificial Intelligence (Ministry of Economic Affairs and Climate Policy, 2019) presents the government's ambition of rolling out AI across its operations. AI can increase efficiency and effectiveness by automating processes and improving service delivery. Yet it also harbours risks such as privacy violations and bias.

An efficient and effective government must use AI responsibly, maximise the opportunities and mitigate the risks. In our opinion, insight into how AI is used is therefore indispensable. Parliament cannot oversee the responsible use of AI if it does not know how the government is using it. This insight is, up to today, lacking. The need to understand how AI is being deployed has become all the more pressing with the entry into force of the AI Act on 1 August 2024. This EU regulation contains requirements regarding the development and use of AI systems and prohibits the use of certain systems in government as from February 2025. To comply with the AI Act, the government must know what AI it is deploying.

This investigation provides an initial insight into the AI central government says it is using, the opportunities government organisations expect AI to deliver and how they assess and mitigate the risks. It follows on from previous investigations by the Court of Audit into the use of algorithms (Netherlands Court of Audit, 2021; 2022; 2023a,b; 2024a,b,c).

## 2.2 Definition of AI

This investigation is based on the definition of AI provided by the AI Act (see box).<sup>1</sup> A key feature of this definition is that AI uses the input it receives to generate outputs. This distinguishes it from other algorithms.

### Definition of AI in the AI Act

“AI system’ means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.”

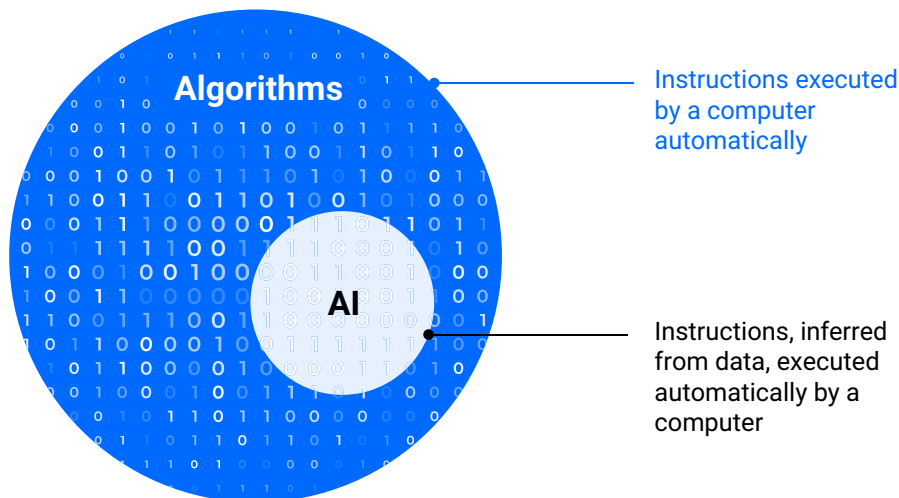
An algorithm is a set of instructions that a computer executes automatically (Netherlands Court of Audit, 2021). By executing the instructions, the computer can make recommendations or answer questions. In many cases, the instructions are specifically programmed into the algorithms. A decision tree, for instance, interprets legal provisions to decide on eligibility for a benefit.

AI by contrast automatically infers the instructions from the input data it receives. Instructions given by programmers are of secondary importance. For instance, an AI system can learn to generate new texts based on existing texts. How it should do so is not specified in advance.

AI systems are algorithms because they automatically execute instructions, but not all algorithms are AI systems. Some algorithms do not infer the instructions from the data (see figure 1). In other words, AI systems are data-driven algorithms.

**Figure 1** Definition of AI

## AI is an algorithm but not all algorithms are AI



## 2.3 AI Act

The AI Act is an EU regulation containing rules on the development and use of artificial intelligence throughout the European Union. The rules apply to all private and public organisations and the Dutch government is no exception. The act follows a risk-based approach, with AI systems being classified into four risk levels:

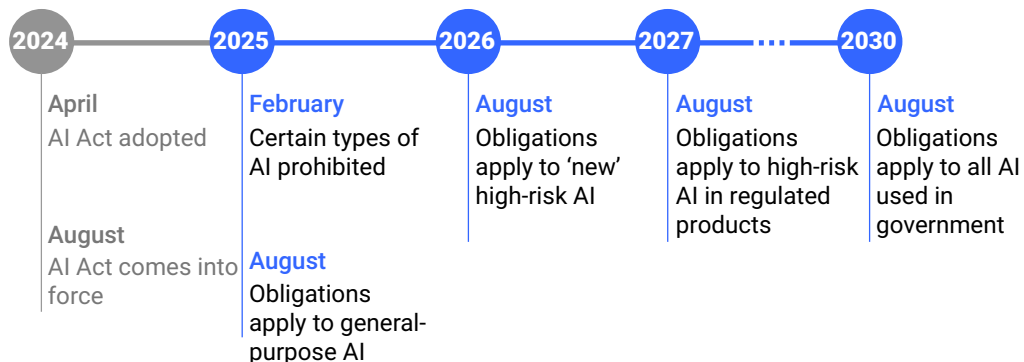
- unacceptable risk<sup>2</sup>
- high risk<sup>3</sup>
- limited risk<sup>4</sup>
- minimal risk.<sup>5</sup>

The higher the risk, the more obligations the development and use of the AI system have to adhere to. We describe this further in §5.2.

Upon the AI Act's entry into force in August 2024, milestones were identified for the years ahead, as shown in figure 2.

**Figure 2** Timeline of government organisations' obligations under the AI Act

### AI systems must comply with the AI Act's requirements in the years ahead



AI systems with an unacceptable risk will soon be subject to the act's obligations. Their use will be prohibited as from February 2025.<sup>6</sup> As from August 2026, the obligations will apply to 'new' AI systems that are used in a high-risk area, such as systems to assess benefit applications. 'New' systems are those taken into use after August 2026. All high-risk AI systems in central government must comply with the AI Act as from 2030. Government organisations must therefore know in advance what AI systems they are using, their risk classification, and what compliance measures they need to take.

## 2.4 Audit approach

To gain an insight into the use of AI in central government, we selected 70 organisations based on their impact on citizens and businesses. The impact can be direct in the form of public services or indirect in a more facilitatory role.

All 70 organisations responded to our request for an inventory of their AI systems. The Ministries of Economic Affairs (EZ), Climate Policy and Green Growth (KGG) and Agriculture, Fisheries, Food Security and Nature (LVVN) completed the questionnaire for their core departments jointly. We therefore refer to 69 organisations in the remainder of this report.

We asked the organisations to complete a questionnaire on their AI systems, both those in current use and those with which they are experimenting or had experimented in the previous 5 years. We asked for a short description of each AI system's status, results and expected risk classification under the AI Act.

In addition to the questionnaire on AI systems, we conducted in-depth interviews with 11 organisations in order to learn about the opportunities and risks they expect from the use of AI.

The investigation focused on the organisational deployment of AI systems. It did not consider the use of AI by civil servants in a personal capacity. AI systems deployed for military or national security purposes also fell outside the scope of the investigation.

Our findings are based on self-reported information from the organisations we selected. Given the nature of the investigation, we did not independently analyse the information's accuracy or completeness.

## Approach

### Focus investigation

This report presents the findings of a focus investigation carried out by the Netherlands Court of Audit. A focus investigation differs from an audit in that it is carried out in a considerably shorter period of time, looks at current events and answers specific, well-defined questions. A focus investigation culminates in a clear, concise report without opinions or recommendations.

See <https://english.rekenkamer.nl/about-the-netherlands-court-of-audit/what-we-do/innovation-in-audit/focus-investigations>

Our methodology is explained in appendix 1. The 70 organisations are listed in appendix 2.

## 2.5 Structure of this report

This report provides an insight into the use of AI by the central government of the Netherlands. Chapter 3 considers the extent to which central government organisations work with AI and for what purpose. Chapter 4 looks at the opportunities and obstacles the organisations see regarding the development and use of AI. Chapter 5 describes how the organisations classify AI systems and mitigate risks.

# 3.

# The use of AI in central government

To gain an insight into the use of AI in the Dutch central government, we asked government organisations to describe the systems they were working or experimenting with. This chapter describes the extent to which they said they were working with AI and for what purpose.

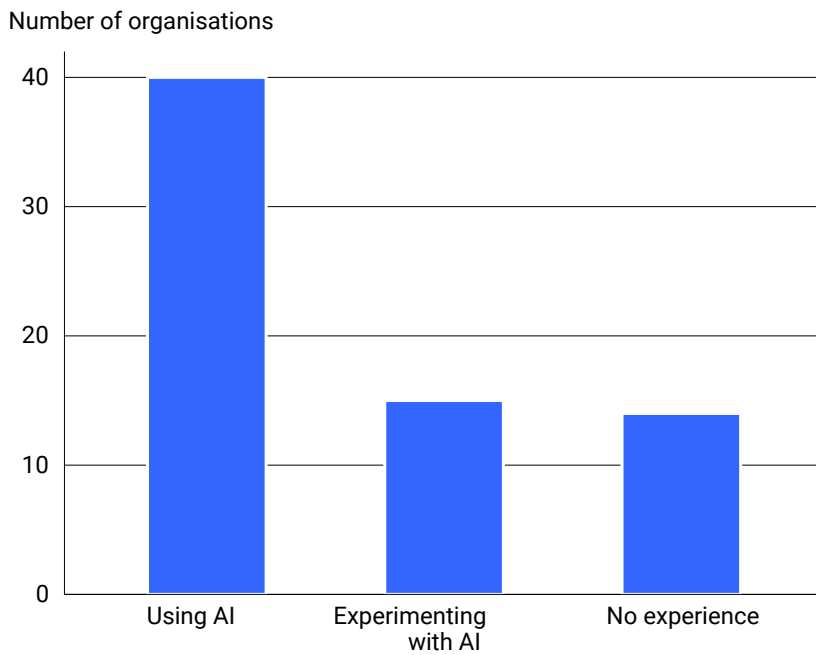
## 3.1 How often is AI deployed?

### **Most organisations use AI**

Most of the organisations surveyed had experience with AI. 40 of the 69 government organisations said they were using AI (see figure 3). For these organisations, AI is a regular element in their business operations. 15 organisations are experimenting with AI but have not yet deployed it. 14 reported they had no experience with AI. Chapter 4 further describes the obstacles preventing government organisations from working with AI.

**Figure 3** Number of organisations investigated that have experience with AI

**Most surveyed organisations use AI**

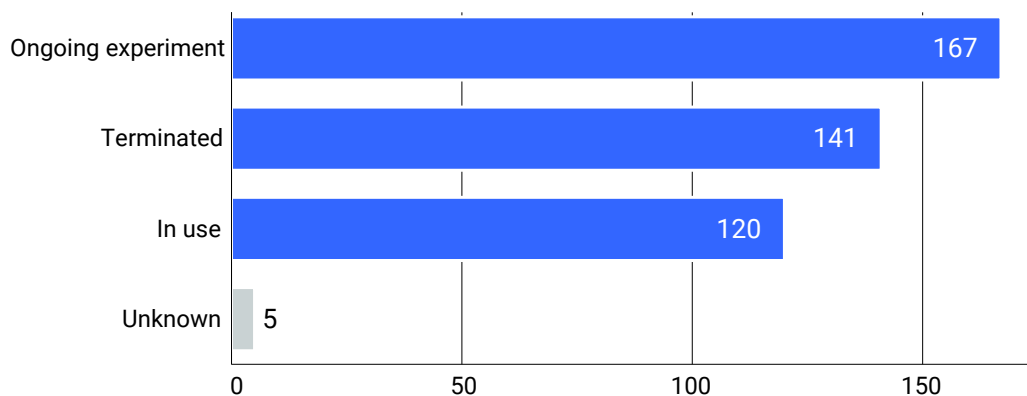


**Most reported AI systems are experiments**

The organisations reported a total of 433 AI systems that were in use, experimental or had been terminated. Figure 4 shows that most of the AI systems are ongoing experiments, either early-stage or advanced.

**Figure 4** Status of AI systems

**Most AI systems are ongoing experiments**



## Few AI systems published in the Algorithm Register

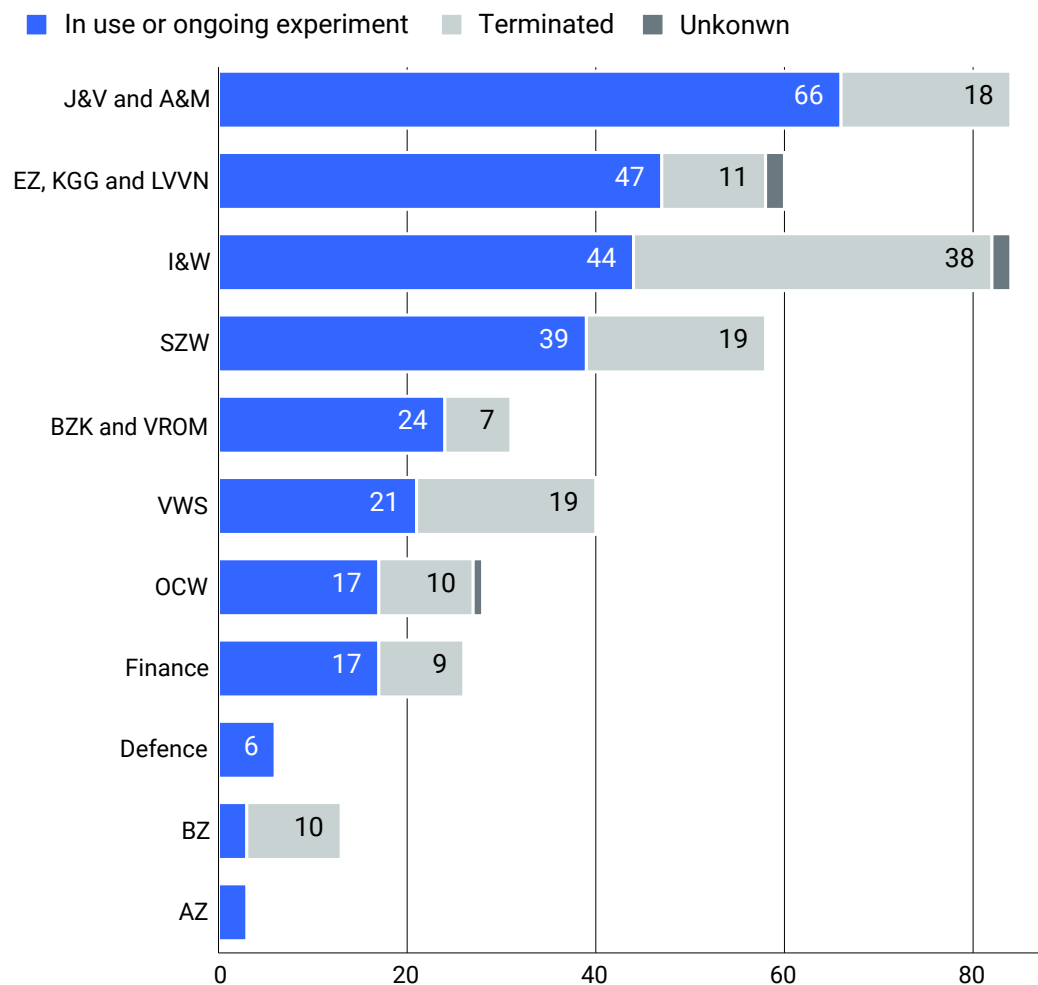
We found that public sources currently provide little information on central government's use of AI. Only 22 (5%) of the 433 reported systems have been entered in the Algorithm Register.<sup>7</sup> Not all AI systems have to be published, but all high-risk systems have to be registered in compliance with the AI Act by 2026.<sup>8</sup> National policy is to have all impactful AI systems published in the Algorithm Register by the end of 2025 (Ministry of the Interior and Kingdom Relations, 2023).

## Numer of AI systems by ministry

Figure 5 shows that most of the AI systems we investigated were deployed by organisations that are part of the Ministries of Justice and Security (J&V), Asylum and Migration (A&M) and Infrastructure and Water Management (I&W).

**Figure 5** Number of AI systems by ministry

### Most AI systems are used by J&V and A&M

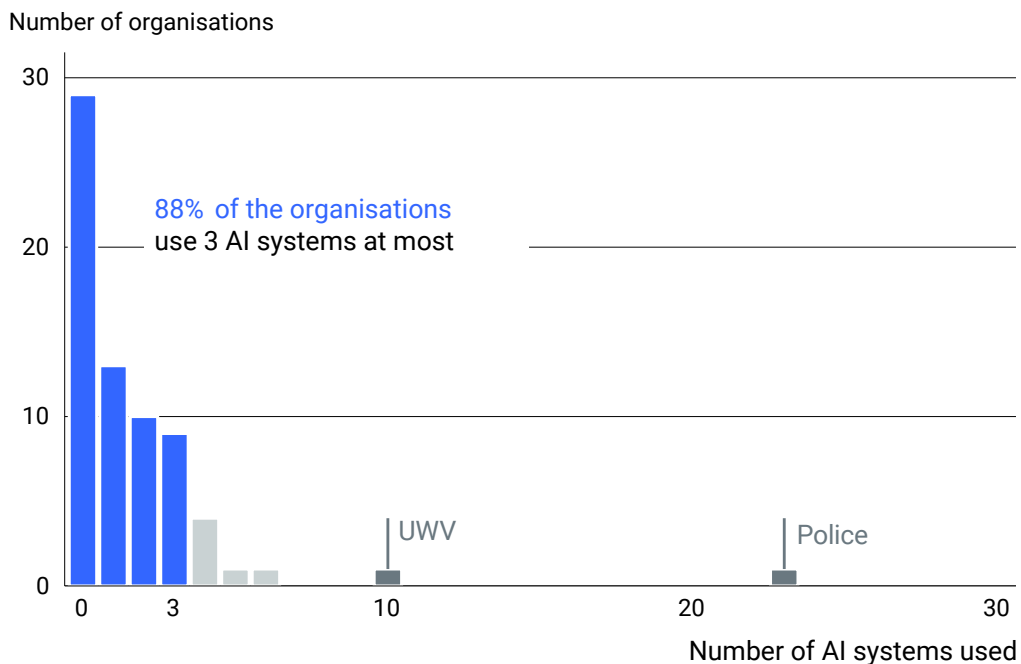


### Most organisations are working with 3 AI systems at most

Of the 433 reported AI systems, the government organisations said 120 were actually in use. Although most of the organisations had already deployed AI, its use per organisation was relatively limited. 88% of the organisations said they were using 3 systems at most (see figure 6). Two organisations stood out: the police and the Employee Insurance Agency (UWV), which were using 23 and 10 AI systems respectively. The police use Slimme Keuzehulp,<sup>9</sup> for example, to help the public report internet scams. The UWV<sup>10</sup> deploys Maatwerkscan to predict who is at risk of having no income when their unemployment benefit ends. It can then offer supplementary support.

**Figure 6** Number of AI systems in use by organisation

#### Government organisations use few AI systems

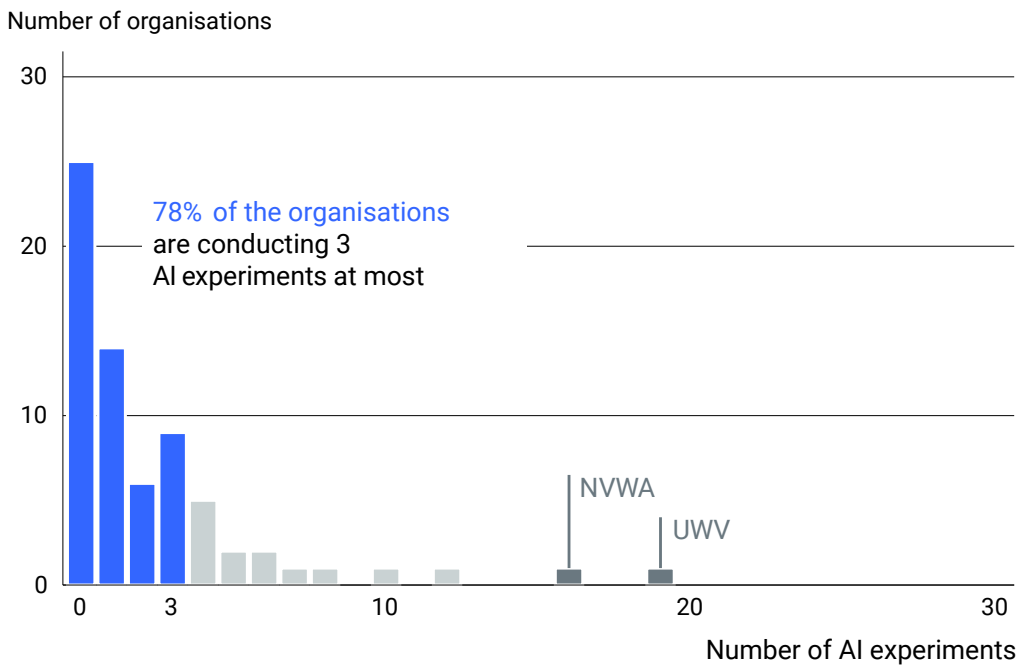


### Most of the AI systems are experiments

The organisations are currently experimenting with AI more than deploying it. Nevertheless, the number of experiments per organisation is also relatively limited. Most organisations said they were conducting 3 AI experiments at most (see figure 7). Two organisations again stood out: the UWV and the Netherlands Food and Consumer Product Safety Authority (NVWA), with 19 and 16 AI experiments respectively. The NVWA, for example, is experimenting with AI to predict fraudulent manure transport.

**Figure 7** Number of AI experiments by organisation

**Few AI experiments per government organisation**










### 3.2 AI applications

**Great diversity in AI applications**

The AI applications in central government are highly diverse. The systems range from antivirus software to search engines and fraud detection systems. From the descriptions given, we divided the AI systems into 9 application types. Figure 8 shows the types and gives examples of the AI systems reported by the organisations. The application types are based on Quicksan AI in Public Services III (TNO, 2024).

**Figure 8** Examples of AI applications in government

### Types of AI applications at government organisations

 <b>Knowledge processing</b>	 <b>Inspection and enforcement</b>	 <b>Process optimisation</b>
<ul style="list-style-type: none"> <li>• Analysing internal documents</li> <li>• Converting speech to text</li> </ul>	<ul style="list-style-type: none"> <li>• Predicting the risk of offences</li> <li>• Checking document compliance</li> </ul>	<ul style="list-style-type: none"> <li>• Assisting in programming of ICT systems</li> <li>• Text writing/editing</li> </ul>
 <b>Knowledge acquisition</b>	 <b>Service delivery</b>	 <b>Monitoring</b>
<ul style="list-style-type: none"> <li>• Identifying social media trends</li> <li>• Predicting staff shortages</li> </ul>	<ul style="list-style-type: none"> <li>• Predicting who will benefit from proactive service delivery</li> <li>• Answering questions from citizens and businesses</li> </ul>	<ul style="list-style-type: none"> <li>• Identifying suspicious behaviour in computer networks</li> <li>• Monitoring news reports</li> </ul>
 <b>Maintenance</b>	 <b>Investigations</b>	 <b>Democratic process</b>
<ul style="list-style-type: none"> <li>• Detecting disruptions</li> <li>• Predicting infrastructure maintenance requirements</li> </ul>	<ul style="list-style-type: none"> <li>• Biometric identification of persons</li> <li>• Identification of objects on photographs</li> </ul>	<ul style="list-style-type: none"> <li>• Processing votes from polling stations</li> <li>• Transcribing parliamentary debates</li> </ul>

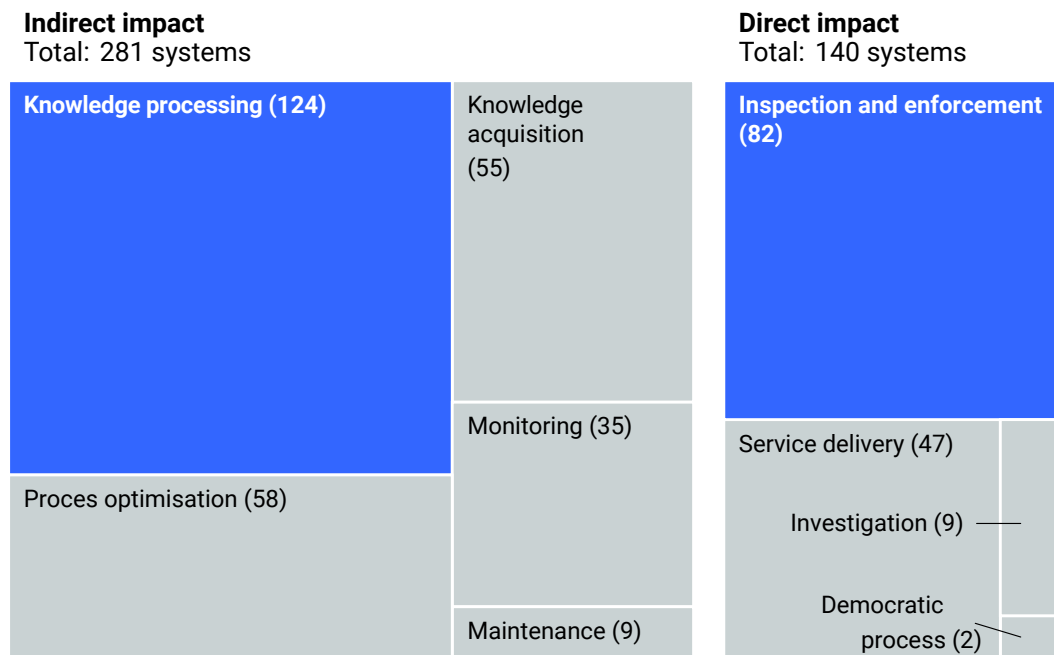
#### AI used mainly for knowledge processing

Figure 9 shows what the AI applications are used for. It is noticeable that government organisations use AI primarily for purposes that do not directly impact citizens and businesses, for instance to acquire and process knowledge or to optimise internal processes.

*Knowledge processing* is the most frequent AI application, with 124 systems. Knowledge processing includes the use of search engines and chatboxes that help analyse internal documents, but also systems to convert speech to text, and software to anonymise documents. The Ministry of General Affairs, for example, uses an AI system to transcribe interviews.

**Figure 9** Number of AI systems by type of application

**AI often used for inspection and enforcement, and knowledge processing**



The use of 12 AI systems could not be determined from the descriptions provided.

A third of the reported AI systems have a direct impact on citizens and businesses, most commonly in *inspection and enforcement procedures* (82 systems). The Custodial Institutions Agency (DJI), for example, is experimenting with a robotic dog to inspect cells. Some inspection and enforcement organisations use AI risk models to predict the risk of future offences based on historical data. The predictions are then used to select citizens and businesses for additional checks. These institutions use AI risk models to select inspection locations or use them to decide whom or what could be subject to additional fraud checks.

The Central Information Point for Healthcare Professions (CIGB) uses an AI system<sup>11</sup> to identify applications to re-register in the Healthcare Professions Register that have a higher risk of non-compliance with the law.

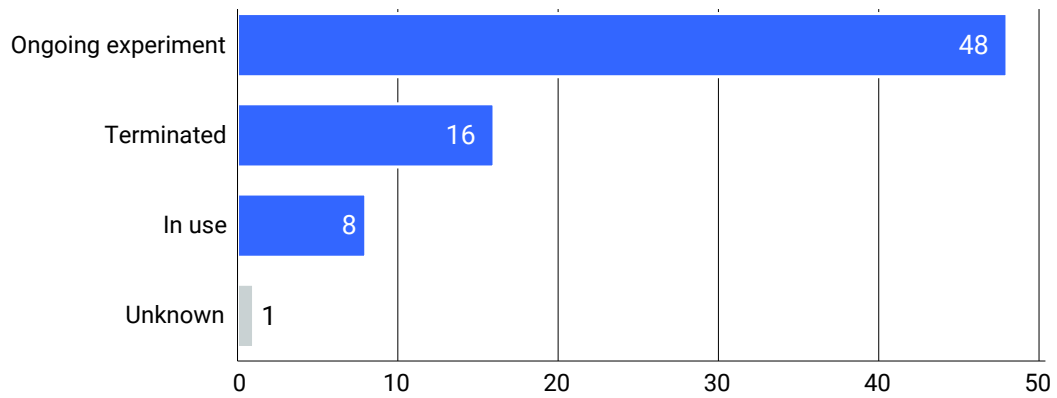
**Generative AI on the rise**

Generative AI is a rapidly emerging AI technique that can create content, such as text, images and videos. Of the 69 surveyed organisations, 29 had had experience with generative AI. In total, they reported 73 generative AI systems. They include chatbots that staff use to ask questions about internal documents, tools to support programmers and systems to write and edit documents. At the moment, most of the reported generative AI systems are experimental (see figure 10).

With 48 experiments and 8 systems in use, generative AI is expected to play a far greater role in central government in the near future.

**Figure 10** *Status of generative AI systems*

**Most generative AI systems are experimental**



# 4.

## Opportunities of AI

**AI offers opportunities for government organisations. It has the potential to increase the efficiency of business processes, improve service delivery and underpin policy-making. This chapter looks at where government organisations think AI's greatest opportunities lie and which obstacles to its use they experience. It also considers the extent to which the organisations think their AI systems fulfilled their expectations.**

### 4.1 Opportunities and results

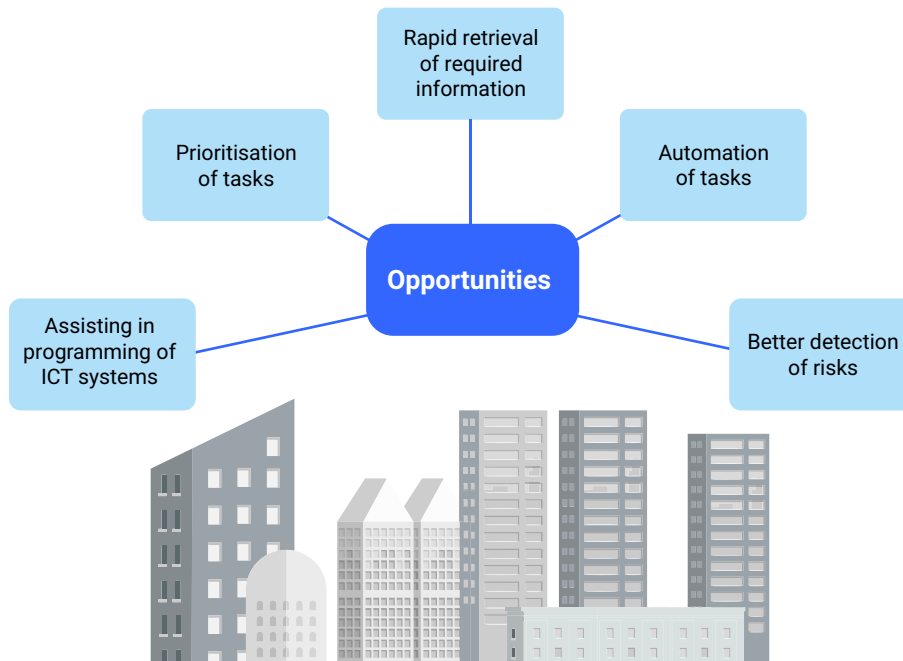
#### **Organisations see opportunities for AI predominantly in process efficiency**

The government organisations we interviewed see opportunities for AI in many areas (see figure 11). They often refer to AI's potential to improve efficiency of internal operations. One of the interviewees said: *'At the moment, [the organisation] thinks AI is particularly opportune in the field of business processes. For example, to categorise information for internal purposes, such as information management, summarising key information, routing workflows and contributing to learning and supporting staff.'*

Some organisations said AI also had the potential to improve checks and monitoring. Other opportunities reported during the interviews were: helping with programming ICT systems, acquiring knowledge and experience, contributing to the scientific field and assisting in the evaluation of other AI systems. Some organisations thought AI could help overcome staff shortages, which may grow in the future.

**Figure 11** *Perceived opportunities of AI*

**Government organisations expect AI to increase the efficiency and effectiveness of work processes**

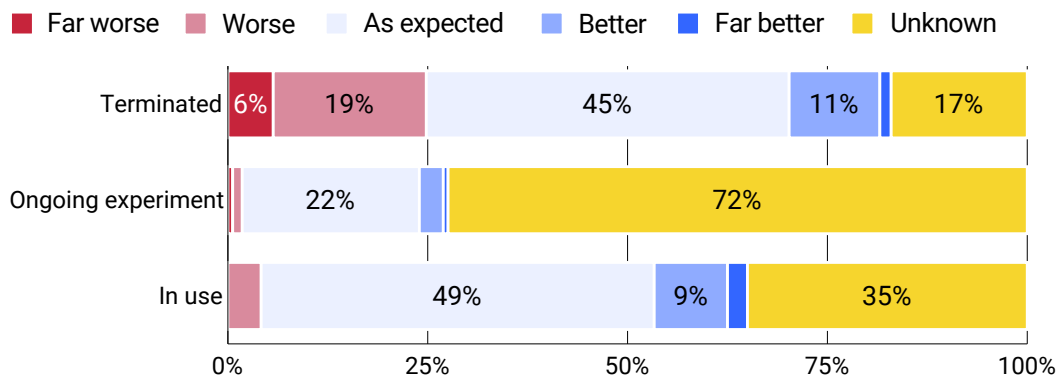


### **Performance of many AI systems unclear**

Interestingly, the organisations often did not know whether their AI systems were actually working as intended. They did not know whether 42 (35%) of the 120 systems in use were living up to expectations (see figure 12). The percentage is even higher among the ongoing experiments (72%). What is also remarkable is that organisations are mostly positive about AI systems they are no longer using, mainly experiments that had been terminated. According to the organisations, 82 of the 141 terminated AI systems (58%) had performed as expected, if not better. In §4.2 we further describe the reasons why government organisations cannot always take advantage of the opportunities AI systems present.

**Figure 12** Expectations of AI systems

**Often unknown what AI systems in use actually achieve**



## 4.2 Obstacles

### Many experiments with AI terminated

Not all AI experiments result in the deployment of an AI system. 121 experiments have been terminated and a further 20 systems were withdrawn after being taken into use. The organisations mentioned various reasons to terminate some systems, ranging from weak predictive power to negative advice from the legal department. In some cases, organisations did not have the necessary capacity to proceed with the experiment.

Some of the organisations we interviewed said they did not mind if an experiment failed to result in a functional AI system. Experimentation was often the first step to decide whether something should be followed up and/or to keep up with the latest developments: *'but even if the outcome is disappointing, an experiment always results in a lesson learned or a new insight'*

### Various obstacles impede AI's development and use

Several organisations said they were not always able to maximise AI's potential. They named various obstacles that hindered the development and use of AI in general. Figure 13 shows the main obstacles.

**Figure 13** Obstacles to the use of AI

**Government organisations name various obstacles to the development and use of AI**



One of the obstacles named by the organisations relates to legislation and regulations. Some organisations said they experienced legal barriers: ‘Regulations are outdated, they offer no possibilities for innovation and data sharing’. The development of AI, they said, was frustrated by ambiguous interpretations of when data could and could not be shared. We have previously referred to the obstacles government organisations face due to the interpretation of privacy legislation in a letter to the House of Representatives.<sup>12</sup>

The organisations also named the IT infrastructure and information management as obstacles to AI’s deployment. One organisation said poor data quality impeded the use of AI: ‘Before we can do fancy things, the basics have to be in order’. Several organisations also said this was why they were not yet using AI. Another said the infrastructure sometimes prevented the use of AI systems. ‘AI systems can only be implemented if the IT platforms are up to the job. This is currently far from being the case’.

The organisations also named human and financial resources as obstacles to AI's development and use. One remarked that knowhow and expertise on AI's opportunities were lacking at all levels in the organisation. It also stated that not enough was known about the preconditions AI and the organisation had to meet. Another organisation said it lacked the capacity to develop and apply AI.

Finally, the organisations said there was a growing compliance burden surrounding the development and use of AI. One organisation thought the increase in the compliance burden was not always proportional: *'Developers spend a lot of time on compliance instead of actually developing AI systems. This can be crippling'*.

# 5.

## AI risks

**The use of AI in government is not without risk, such as bias and privacy violations. The explainability of AI also entails risks. In comparison with rule-based algorithms, AI is often difficult to understand and it is not always clear why the system takes a particular decision.**

**To use AI responsibly, organisations must weigh up the opportunities and benefits against the risks. To meet the requirements of the AI Act, they must know which of its risk classifications apply to their systems.**

**This chapter describes the extent to which the government organisations have assessed the risks of their AI systems. It also looks at the risk categories the organisations think apply to their systems and the risk management implications.**

### 5.1 Risk management

#### **AI risk management often part of the general risk management process**

Several government organisations we interviewed stressed the importance of risk assessment when deploying AI. One organisation asked: *'When do you deploy AI? Which applications are valuable and have an acceptable risk? Wherever possible, we take an integrated approach involving multiple parts of the organisation'*.

Some of the organisations said they had drawn up policy or guidelines on the development and use of AI. The risk management of AI is often embedded in the existing regular risk management process, for instance, for information security and privacy, and is not AI specific.

One organisation said: *'The risk management department has set up a strict risk management process for IT systems. It decides which additional AI management measures should be added to the process. One of the expert group's recommendations is to include additional AI management measures in the regular risk management process.'*

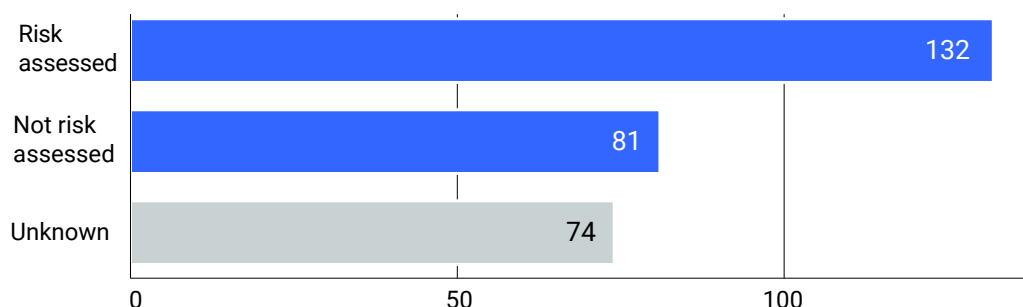
Most organisations we interviewed said they were still formulating and tailoring their risk management to the AI Act. One organisation explained: *'The CDO Office is working out policy, rules and guidelines for data, AI and algorithms. It has already presented guidance on how [the organisation's] staff should use generative AI that is already publicly available. The CDO Office is also drafting a policy document on responsible use of AI.'*

### **Not all AI systems have been risk assessed**

We asked whether the organisations had carried out a documented risk assessment before or during their use of AI. They replied that they made a risk assessment for fewer than half of their systems (see figure 14). This relates to 132 (46%) of the 287 reported AI systems that are either currently in use or are ongoing experiments. These findings do not include discontinued AI systems. For 155 systems, the organisations said they had not made a risk assessment or they did not know. For this investigation, we did not validate or substantively test the risk assessments that had been carried out.

**Figure 14** Risk assessment of AI systems

#### **Not all AI systems underwent a risk assessment**



This figure presents information on only the 287 AI systems currently under development or in use.

Some organisations said they had not carried out a risk assessment because their AI systems were at an early stage of development. *'We don't know precisely how the AI will work or what data it will use. We'll figure this out during the pilot and then carry out a risk assessment when we know'*. Several organisations said they would make a risk assessment when they decided to put an AI system into use.

Others said a risk assessment had not been made, or it was unknown, because the AI system used only public information or did not process personal details.

### Wide range of risk assessment instruments

A wide range of instruments are used to assess an AI system’s risks. They include a Fundamental Rights and Algorithms Impact Assessment (FRAIA) and a Data Protection Impact Assessment (DPIA) but many other tools are also available. The great variety of risk assessment instruments used by the organisations is shown in table 1.

**Table 1** Risk assessment instruments for AI systems

Type	Instruments used
Algorithms/AI frameworks	Netherlands Court of Audit Algorithm Assessment Framework Algorithms Manual Algorithms Implementation Framework Fundamental Rights and Algorithms Impact Assessment (FRAIA) EU AI Act Compliance Checker AI Impact Assessment
Privacy frameworks	Data Protection Impact Assessment (DPIA) Machine learning addendum to existing DPIA Privacy check
Other frameworks	Ethical check Ethical Impact Assessment (EIA) Information security risk assessment General Security Requirements relating to Defence Orders (ABDO) Data Governance Act Impact Analysis (DGA) Cloud assessment framework Business case
Quickscans	Information security quickscan Government Information Security Baseline (BIO) quickscan DPIA quickscan Pre-DPIA Accelerated FRAIA Algorithm checklist AI risk scan Assessment of main features

Most of the risk assessments that had been carried out were privacy assessments in the form of a DPIA<sup>13</sup> or Data Protection Impact Assessments (DPIA).<sup>14</sup> Other risk assessments included specific algorithm or AI frameworks, ranging from the Court of Audit’s Algorithm Assessment Framework<sup>15</sup> and the Algorithms Implementation Framework<sup>16</sup> to FRAIAs.<sup>17</sup> Some organisations named AI-related risk assessments, such as the AI Impact Assessment.<sup>18</sup> Some mentioned other assessment frameworks, such as ethical checks, a cloud assessment framework, and risk assessments for information security or a business case.

Some risk assessments were quickscans or considered only a system's main features.

There is no government-wide instrument to assess AI risks. A few organisations have developed their own AI risk assessment instruments. One organisation said that for several systems it had developed and applied its own impact assessment framework *'based on the Ministry of BZK's algorithms guideline and the Algorithms Implementation Framework'*. Another said FRAIAs were inappropriate for its AI system and had therefore applied its own algorithm framework based on the Algorithms Implementation Framework.

Many organisations said comprehensive assessment of an AI system cost a lot of time and there was uncertainty about when the results of the assessment were good enough. They therefore worked with shorter quickscans to gain an indication of the risk before deciding on a comprehensive risk assessment: *'It begins with a quickscan to give an indication of the rest of the process: a low risk leads to fewer quality-based requirements (such as the periodicity of risk assessment) than a high risk'*.





## 5.2 Risk classification

### **Risk classification has consequences for the risk management process**

The AI Act (see §2.3) imposes obligations on AI systems in Europe. The more risks an AI system has, the more rules apply to it. Figure 15 describes the risk categories in the AI Act and related obligations.

**Figure 15** AI Act obligations applying to AI systems

### The four risk classifications of the AI Act

-  **Unacceptable risk**  
Use of AI systems with unacceptable risk prohibited as from 1 February 2025.
-  **High risk**  
Government organisations must meet strict requirements regarding the use of high-risk AI systems.
-  **Limited risk**  
Government organisations must transparently inform users if they are working with an AI system with limited risk.
-  **Minimal risk**  
AI systems with minimal risk are systems that do not fall into one of the above categories.

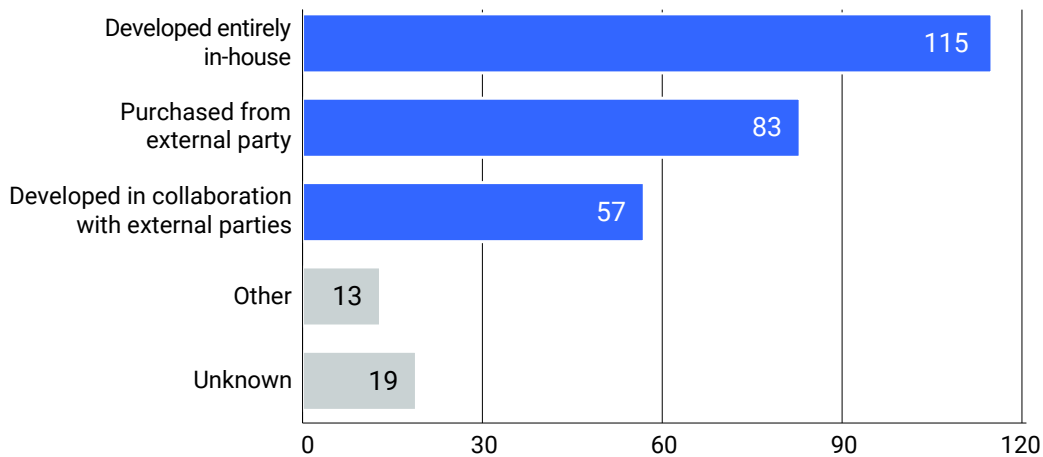
The risk classification has many consequences for the risk management process. All high-risk AI systems must meet the strict requirements of the AI Act in due course.<sup>19</sup> Under the AI Act, systems with limited risk must comply only with transparency obligations,<sup>20</sup> such as informing users that they are using an AI system. AI systems with minimal risk can be used without having to satisfy further obligations under the AI Act. This might induce organisations to give their systems a lower risk classification.

#### **Most AI systems have been developed entirely in-house**

The AI Act makes a distinction between the providers of AI systems and the parties responsible for their deployment. In general, the provider develops the system and is thus responsible for its correct classification. The provider must also ensure that the system satisfies most of the obligations applying under the AI Act. We asked the organisations to tell us who had developed each of their AI systems.

**Figure 16** *Developer of the AI system*

**Most AI systems are developed entirely in-house**



This figure presents information on only the 287 AI systems currently under development or in use.

Most of the current and experimental AI systems were developed entirely in-house (see figure 16). The government organisations themselves are therefore responsible for the systems' correct classification and their satisfaction of all the AI Act's obligations. The organisations classified 17 of the 115 systems developed in-house as high risk. In due course, these systems must meet the AI Act's many strict requirements.

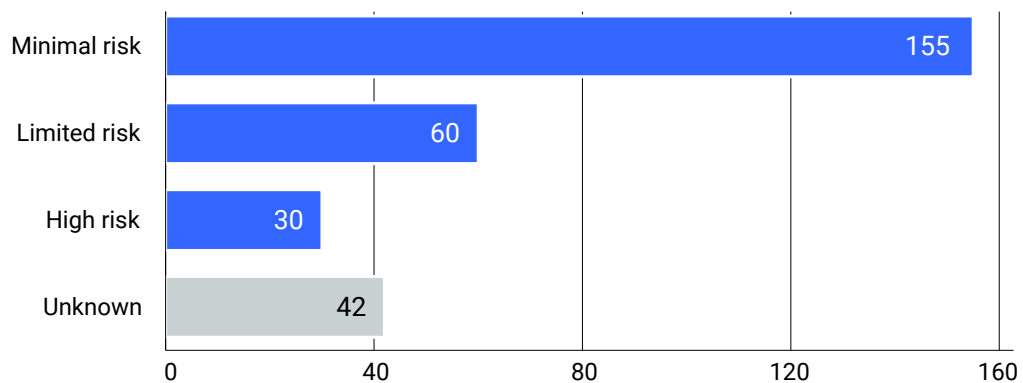
A smaller but still considerable proportion of the AI systems had been bought from third parties. They include systems developed by an external provider, sometimes as part of an AI application or existing software package. One organisation we interviewed said it was concerned about the potential, often unknown, risk exposure when buying from an external provider: *'More and more ICT systems have a substantial AI component. There is a real risk you'll be buying AI without knowing it.'*

**Organisations classify most AI systems as minimal risk**

The organisations we surveyed had classified most of their AI systems and experiments as minimal risk (155) or limited risk (60), as defined in the AI Act (see figure 17). Under the AI Act, few if any requirements apply to these systems.

**Figure 17** Organisations' estimates of their AI systems' risk classification

**Organisations classify most of their AI systems as minimal risk**



This figure presents information on only the 287 AI systems currently under development or in use.

Nevertheless, AI systems classified as minimal or limited risk can still harbour risks such as privacy violations, weak information security or negative impact on citizens and businesses, e.g. unfair biases. Furthermore, AI systems with minimal or limited risk must comply with statutory and regulatory provisions such as the General Data Protection Regulation (GDPR). All the government's systems must also satisfy the Government Information Security Baseline (BIO).

**No systems in use with unacceptable risk, say the organisations**

The organisations say they are not using prohibited AI systems. It is thought, however, that 2 of the reported systems, neither of which is still in use, would have been prohibited under the AI Act as they represented an unacceptable risk. Some organisations we interviewed said they were uncertain whether they were using systems that had an unacceptable risk. Since these systems will be prohibited as from February 2025, it is exceedingly important that the organisations find out soon.

**High-risk AI systems**

The organisations say they are currently using or developing 30 systems in total that they think will be high risk under the AI Act. The AI systems classified as high risk include:

- a system that automatically compares fingerprints and handprints to establish or verify a person's identity;
- a migration-related system for legal translators that automatically transcribes and translates interviews ;
- a system that predicts who is more likely to have problem debts and can be proactively offered debt counselling;
- a system that can detect, investigate and respond to digital security threats.

High-risk AI systems in use or that will be used in the near future must meet strict requirements regarding risk management, data quality, transparency, accuracy and robustness. Government organisations that use these systems must carry out a fundamental rights check to identify the consequences.<sup>21</sup>

### **Risk classification still being developed**

Several organisations said risk classification of their AI systems was a work in progress. One said it had not yet agreed on a definitive classification: *'We have classified relatively simple AI and AI that doesn't have an external impact as "minimal" and advanced image and text processing algorithms as "limited". When we get round to the actual classification, we expect we'll have to reclassify some systems.'* Another organisation explained that interpretation of the AI Act was also a work in progress: *'Interpretation of the AI Act is subject to change. Based on our interpretation of the current text, [the AI system] is minimal risk. Others have a different interpretation and we'll consult them to see if we should reconsider ours.'*

The uncertainty of the risk classification of AI systems is reflected in the reported AI systems and their risk levels: 3 organisations that use an AI system to compare fingerprints classify it in 3 different ways: minimal, limited and high. Such differences arise if the organisations use the systems for different purposes. The AI Act's risk classification based on the system's application, not the system itself.

# 6. Response

We sent our draft report to the State Secretary for the Interior and Kingdom Relations (BZK), who responded in his capacity as coordinator of the digitalisation of the Dutch government. His response gives us no cause for an afterword. The state secretary's letter is available (in Dutch) on our website ([www.rekenkamer.nl](http://www.rekenkamer.nl)).

# Appendices

## Appendix 1 Methodology

This aim of this investigation is to provide an insight into the use of AI in the Dutch central government, the opportunities organisations foresee for it and how they assess and mitigate the risks. This appendix describes what we investigated and how we did so.

### What did we investigate?

#### Key question

What insight does the Dutch central government, and the organisations associated with it, have into the use of AI systems?

To answer this key question, we asked the following sub-questions:

1. What AI systems are currently in use at selected government organisations?
2. What AI experiments are being carried out or have been carried out?
3. What are the opportunities of AI systems and are they being achieved?
4. How are the risks of AI assessed and mitigated?

The findings in this report are based on information self-reported by the government organisations we selected. We did not independently analyse the accuracy or completeness of the information. Similarly, additional information on each AI system was self-reported by the organisations we selected. We did not carry out additional analyses of the descriptions and assessments.

## Approach

### Focus investigation

This report presents the findings of a focus investigation carried out by the Netherlands Court of Audit. A focus investigation differs from an audit in that it is carried out in a considerably shorter period of time, looks at current events and answers specific, well-defined questions. A focus investigation culminates in a clear, concise report without opinions or recommendations.

See <https://english.rekenkamer.nl/about-the-netherlands-court-of-audit/what-we-do/innovation-in-audit/focus-investigations>

### What do we understand under AI?

This investigation is based on the definition of AI given in the AI Act: ‘a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments’.

In brief, for the purpose of the investigation we take AI to mean data-driven algorithms. We do not consider rule-based systems such as simple decision trees or simple automation to be AI. The main difference between AI within the meaning of this report and rule-based systems is that AI infers how to perform tasks from data instead of being specifically programmed to perform those tasks. Rule-based systems are algorithms but we did not consider them to be AI in this investigation.

We did not investigate AI applications that civil servants used on an ad hoc and individual basis, such as a personal ChatGPT account. Neither did we investigate AI used for military, defence or national security purposes.

### Selection of organisations

For this investigation, we requested an inventory of the AI systems in use at 70 organisations across central government. The organisations are listed in appendix 2. We selected the organisations based on their impact on citizens and businesses. The impact can be direct, in the form of service delivery, or indirect, in a more facilitative role. The investigation covered 69 organisations, as the Ministries of Economic Affairs (EZ), Climate Policy and Green Growth (KGG) and Agriculture, Fisheries, Food Security and Nature (LVVN) completed the questionnaire jointly for their core departments.

## **Analysis**

We asked all 70 organisations to list the AI systems their organisations were using and to complete a questionnaire for all systems in use, ongoing AI experiments and AI experiments/pilots terminated or paused in the past 5 years, for instance in anticipation of being taken into production. The inventories were checked for empty fields. Where columns had not been completed, we contacted the organisation concerned for further information.

## **Interviews**

We held additional in-depth interviews at 11 organisations to gain an insight into the opportunities and risks they expected of their use of AI. The organisations we selected for interview are listed in appendix 2.

## Appendix 2 Selected organisations

The table below lists the organisations we selected for our investigation of AI systems.

The Ministries of Housing and Spatial Planning (VRO), Climate Policy and Green Growth (KGG) and Asylum and Migration (A&M) had not been established at the time of our investigation. They were part of other ministries, as show in the table below.

\* We have placed an asterisk (\*) next to the 11 organisations that we interviewed in-depth.

\*\* The Ministries of Economic Affairs (EZ), Climate Policy and Green Growth (KGG) and Agriculture, Fisheries, Food Security and Nature (LVVN) completed the questionnaire for their core departments jointly.

### Ministry of General Affairs (AZ)

Organisation	Status
AZ core department	Part of the ministry

### Ministry of the Interior and Kingdom Relations (BZK) and Ministry of Housing and Spatial Planning (VRO)

Organisation	Status
BZK and VRO core department	Part of the ministry
Logius	Agency
National Office for Identity Data (RvIG)	Agency
SSC-ICT	Agency
Central Government Real Estate Agency (RVB)	Agency
Electoral Council	Autonomous Administrative Authority (ZBO)
Rent Tribunal	ZBO
Land Registry	ZBO/ Legal person with statutory tasks (RWT)

### Ministry of Foreign Affairs (BZ)

Organisation	Status
BZ core department	Part of the ministry

### Ministry of Defence (Def)

Organisation	Status
Def* core department	Part of the ministry

### Ministry of Economic Affairs (EZ), Ministry of Climate Policy and Green Growth (KGG) and Ministry of Agriculture, Fisheries, Food Security and Nature (LVVN)

Organisation	Status
EZ, KGG and LVVN** core department	Part of the ministry
ICT Services (DICTU)	Agency
Netherlands Enterprise Agency (RVO)*	Agency
Authority for Consumers and Markets (ACM)	ZBO
Chamber of Commerce (KvK)	ZBO/RWT
Netherlands Food and Consumer Product Safety Authority (NVWA)*	Agency

### Ministry of Finance (Fin)

Organisation	Status
Fin core department	Part of the ministry
Tax and Customs Administration*	Part of the ministry
Customs	Part of the ministry
Benefits Office	Part of the ministry

### Ministry of Infrastructure and Water management (I&W)

Organisation	Status
I&W core department	Part of the ministry
Human Environment and Transport Inspectorate (ILT)	Part of the ministry
Royal Netherlands Meteorological Institute (KNMI)	Agency
Rijkswaterstaat	Agency
CBR	ZBO/RWT
Air Traffic Control The Netherlands (LVNL)	ZBO/RWT
RDW	ZBO/RWT
ProRail	RWT

## Ministry of Justice and Security (J&V) and Ministry of Asylum and Migration (A&M)

Organisation	Status
J&V and A&M core department	Part of the ministry
Public Prosecution Service (OM)	Part of the ministry
Childcare Protection Board	Part of the ministry
Repatriation and Departure Service (DT&V)	Part of the ministry
Central Judicial Collection Agency (CJIB)	Agency
Custodial Institutions Agency (DJI)	Agency
Integrity and Screening Agency (Justis)	Agency
Judicial ICT Organisation (JIO)	Agency
Judicial Information Service (Justid)	Agency
Netherlands Forensic Institute (NFI)*	Agency
Immigration and Naturalisation Service (IND)	Agency
National Maintenance Collection Agency (LBIO)	ZBO/RWT
Legal Aid Board	ZBO/RWT
Legal Aid and Advice Centre	RWT
Police*	RWT
Victim Support Netherlands	RWT
Halt*	RWT
Central Agency for the Reception of Asylum Seekers (COA)	ZBO

## Ministry of Education, Culture and Science (OCW)

Organisation	Status
OCW core department	Part of the ministry
Inspectorate of Education	Part of the ministry
Education Executive Agency (DUO)	Agency
National Library of the Netherlands (KB)	ZBO/RWT
NPO	ZBO
Cito	RWT

## Ministry of Social Affairs and Employment (SZW)

Organisation	Status
SZW core department	Part of the ministry
Arboportaal	Part of the ministry
Labour Inspectorate	Part of the ministry
Social Insurance Bank (SVB)*	ZBO/RWT
Employee Insurance Agency (UWV)	ZBO/RWT
Benefits Intelligence Agency	RWT

## Ministry of Health, Welfare and Sport (VWS)

Organisation	Status
VWS core department	Part of the ministry
Health and Youth Care Inspectorate (IGJ)	Part of the ministry
Youth Authority	Part of the ministry
Implementing Agency for Grants to Institutions (DUS-I)*	Part of the ministry
Central Information Point for Healthcare Professions (CIBG)	Agency
National Institute for Public Health and the Environment (RIVM)*	Agency
Medicines Evaluation Board Agency (aCBG)	Agency
CAK	ZBO/RWT
Medicines Evaluation Board (CBG)	ZBO
CIZ	ZBO/RWT

## Appendix 3 Literature

Netherlands Court of Audit (2021), *Understanding algorithms*, The Hague, self-published.

Netherlands Court of Audit (2022), *An audit of algorithms*, The Hague, self-published.

Netherlands Court of Audit (2023a), *Results of the Accountability Audit 2022, Ministry of Justice and Security*, The Hague, self-published.

Netherlands Court of Audit (2023b), *Results of the Accountability Audit 2022, Ministry of Social Affairs and Employment*, The Hague, self-published.

Netherlands Court of Audit (2024a), *Results of the Accountability Audit 2023, Ministry of Defence*, The Hague, self-published.

Netherlands Court of Audit (2024b), *Results of the Accountability Audit 2023, Ministry of Infrastructure and Water Management*, The Hague, self-published.

Netherlands Court of Audit (2024c), *Results of the Accountability Audit 2023, Ministry of Justice and Security*, The Hague, self-published.

Ministry of the Interior and Kingdom Relations (2023), *Letter from the State Secretary for the Interior and Kingdom Relations*, Parliamentary Paper 26 643, no. 1056.

Ministry of Economic Affairs and Climate Policy (2019), *Strategic Action Plan for Artificial intelligence*,  
[https://wp.oecd.ai/app/uploads/2021/12/Netherlands\\_Strategic\\_Action\\_Plan\\_for\\_Artificial\\_Intelligence.pdf](https://wp.oecd.ai/app/uploads/2021/12/Netherlands_Strategic_Action_Plan_for_Artificial_Intelligence.pdf)

TNO (2024). *Quickscan AI in Public Services III*.  
<https://publications.tno.nl/publication/34642601/SASNc3ZW/TNO-2024-R11005.pdf>

## Appendix 4 Endnotes

1. AI Act, article 3 (1).
2. Prohibited AI practices are described in article 5 of the AI Act. See also <https://www.nldigitalgovernment.nl/featured-stories/which-ai-practices-will-be-banned-next-year/>
3. The classification rules for AI systems are described in article 6 of the AI Act. Annex III of the AI Act lists the areas that are considered high risk.
4. The European Commission uses the term 'limited risk' to refer to AI systems subject to additional transparency obligations (<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>). Article 50 of the AI Act explains which AI systems are subject to additional transparency obligations and what those obligations are.
5. These are AI systems that do not fall into the AI Act's other classifications.
6. Prohibited AI practices are described in article 5 of the AI Act. See also endnote 2.
7. The Dutch government's Algorithm Register: <https://algoritmes.overheid.nl/en>.
8. AI Act, article 49.
9. Slimme Keuzehulp AI system: <https://aangifte.politie.nl/iaai-preintake/>
10. Maatwerkscan AI system: <https://www.uwv.nl/nl/over-uwv/organisatie/algoritmeregister-uwv/maatwerkscan>
11. BIG re-registration selection model AI system: <https://algoritmes.overheid.nl/en/algoritme/big-reregistration-selection-model-cibg/59917797>
12. Netherlands Court of Audit (2023), GDPR and the performance of government tasks: <https://www.rekenkamer.nl/publicaties/kamerstukken/2023/03/30/omgang-met-de-avg-in-relatie-tot-uitvoering-overheidstaken>
13. Data Protection Impact Assessment (DPIA): <https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/praktisch-avg/data-protection-impact-assessment-dpia>
14. Data protection impact assessment (DPIA): <https://open.overheid.nl/documenten/ronl-8ea75bee-4f37-42f0-98c9-718929aaeafc/pdf>
15. Netherlands Court of Audit, Algorithm Assessment Framework: <https://english.rekenkamer.nl/publications/publications/2021/01/26/audit-framework-for-algorithms>
16. Implementation framework for the responsible use of algorithms: <https://www.rijksoverheid.nl/documenten/rapporten/2023/06/30/implementatiekader-verantwoorde-inzet-van-algoritmen>

17. Fundamental Rights and Algorithms Impact Assessment:  
(<https://www.government.nl/documents/reports/2021/07/31/impact-assessment-fundamental-rights-and-algorithms>)
18. AI Impact Assessment: <https://www.government.nl/documents/publications/2023/03/02/ai-impact-assessment>
19. Articles in sections 3, section 5 and other sections of the AI Act lay down the requirements that high-risk AI systems must meet.
20. See AI Act, article 50
21. Government organisations that use high-risk AI systems must assess fundamental rights consequences. The requirements are stated in article 27 of the AI Act.

**Netherlands Court of Audit**

PO Box 20015

2500 EA The Hague

The Netherlands

Phone +31 70 342 44 00

[voorlichting@rekenkamer.nl](mailto:voorlichting@rekenkamer.nl)

[www.courtofaudit.nl](http://www.courtofaudit.nl)

Photo cover: ANP/Hollandse Hoogte/  
Sandra Uittenbogaart

**The Hague, October 2024**