Comparative Legal Study on AI System Certification:

Current Status and Future Challenges Across Jurisdictions

Kyoto University Graduate School of Law
Center for Interdisciplinary Studies of Law and Policy (KILAP)

Hiroki Habuka (KILAP, Research Professor)

Socol de la Osa David Uriel (Hitotsubashi Institute for Advanced Study, Assistant Professor)

Kei Takahashi (PhD Candidate at Kyoto University, Attorney at Law)

Index

Introduction 3
Purpose of This Report 3
Background of This Study and Scope of This Report 4
Structure of This Report 5
1. Structure of Certification 6
(1) Conventional Certification Frameworks 6
(i) Product Certification 6
(ii) Management System Certification 6
(iii) Operator Certification 6
(2) Challenges in Certifying AI 7
2. Comparative Analysis of Certification Frameworks Across Jurisdictions 9
(1) Autonomous Vehicles 9
(i) Japan 9
(ii) United States 11
(iii) EU 12
(iv) United Kingdom 15
(2) Medical Devices 18
(i) Japan 18
(ii) United States 20
(iii) EU 21

(iv) United Kingdom....23
3. Key Findings and Challenges in AI Certification....26
(1) Key Findings from Comparative Analysis....26
(i) Autonomous Vehicles....26
(ii) Medical Devices....26
(2) Future Challenges....27
(i) Institutional Framework for AI Certification....27
(ii) Certification Methods....28
(iii) Certification Bodies....29
(iv) Relationship Between Certification and Liability Regimes....29
Appendix 1: Preliminary Survey on Legal Certification Systems across Jurisdictions....30
1. Summary of Survey....30
2. Survey Results....31
Appendix 2: European Union: Overview of AI Act Requirements for High-Risk AI Systems....43

Introduction

Purpose of This Report

In recent years, AI systems[1] have attained performance levels comparable to or even surpassing humans in numerous tasks, leading to their replacement of certain human roles in various sectors. Consequently, there is growing anticipation for certification as a means to ensure trust in AI systems. Certification means a formal process in which an independent body evaluates and verifies that a product, process, service, or system meets specified requirements or standards.[2] AI systems exhibit unique characteristics, including high autonomy, significant influence on human decision-making, and unpredictability or limitation of explainability due to complex machine learning. These attributes make it inherently difficult for third parties to assess their safety and reliability. As a result, the need for independent experts to certify AI systems and objectively guarantee their trustworthiness is even greater than for conventional systems. However, these very characteristics of AI systems also introduce challenges in certification that do not exist for conventional systems.

Conventional certification has generally applied to products, processes, or systems (such as waterfall systems) that are clearly defined and operate within predictable parameters and established frameworks. It relies on precise and measurable criteria to ensure safety, quality, and reliability, and is implemented with a clear understanding of associated risks. For example, in the case of conventional automobiles or medical devices, certain threshold values are set for their performance and safety—such as crash resistance for automobiles or efficacy for medical devices—allowing for direct risk assessment and evaluation of mitigation measures.

In contrast, AI systems differ from conventional technologies in that they autonomously construct highly complex algorithms based on training data. As a result, their behavior is virtually impossible to predict or explain, making it difficult to establish uniform reliability assessment criteria. Additionally, the range of risk scenarios and uncertainties to be addressed is significantly broader, such as the infinite traffic situations faced by autonomous vehicles or unforeseen medical complications arising from AI-assisted medical devices. Furthermore, AI systems function by integrating diverse elements, including data, software, hardware, and human interactions. The interplay among these multiple components can introduce risks that are not predictable based solely on the functions of individual systems.

This report aims to conduct a cross-jurisdictional comparison of legal frameworks for AI system certification, extract common institutional structures and issues to be discussed across different fields and countries, and provide insights into Japan's approach to AI licensing and the feasibility of international cooperation on this matter.

---

[1] Regarding the definition of AI, we follow the definition presented by the OECD: "An AI system is a machine-based system 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. Different AI systems vary in their levels of autonomy and adaptiveness after deployment."

[2] https://www.iso.org/certification.html

Background of This Study and Scope of This Report

For the preparation of this report, we first conducted a preliminary study on legal frameworks for AI system certification across various sectors, including mobility (autonomous vehicles), healthcare, finance, legal services, generative AI (GenAI), and labor. The study covered Japan, the EU, the United States (US), the United Kingdom (UK), Canada, Singapore, and China (see **Appendix 1**), as of August 2024. While certification is often obtained voluntarily as part of private-sector initiatives rather than as a legal obligation, this study focuses on legally mandated certifications. By doing so, we aim to conduct a comparative analysis of certification processes that have been established through legislative procedures.

The preliminary study confirmed that all the surveyed countries and regions have certification systems in place for AI systems used in **autonomous vehicles and medical devices**. In contrast, only a few jurisdictions have introduced certification systems specifically for AI systems used in finance, legal services, and labor. Similarly, in the case of generative AI, legislative action has been observed primarily in the EU and China, while other countries have yet to implement specific legal frameworks.

Several factors likely explain why certification systems have developed particularly in the fields of **autonomous vehicles (AVs) and medical devices (MDs)**: (i) the rapid adoption of AI technologies in these sectors, (ii) the inherently high-risk nature of these fields, where erroneous AI decisions could have severe consequences for human life and safety, and (iii) the existence of well-established certification systems for these products even before the advent of AI. Given these factors, this report focuses on the comparative analysis of certification systems for AVs and MDs across jurisdictions.

As for the jurisdictions covered in this report, we selected **Japan, the US, the EU, and the UK**. These four jurisdictions are all members of the G7, democratic, and technologically advanced, making them valuable points of reference for Japan's institutional comparison. Regarding the **EU**, its AI Act extends certification (conformity assessment) beyond conven-tional domains like AVs and MDs to a broader range of "high-risk AI systems." In addition to a summary of this general certification framework, **Appendix 2** provides an explanation of the scope of application of the AI Act to AVs and MDs. Meanwhile, although China has been actively developing its own regulatory framework, its political system differs significantly from that of the four jurisdictions mentioned above. For this reason, China is not included in the cross-jurisdictional comparison in this report.

To summarize, the main body of this report examines the following aspects:

- **Objective:** Comparative analysis of legally mandated AI system certification frameworks
- **Target Sectors:** AVs and MDs equipped with AI as their core functionality
- **Target Jurisdictions:** Japan, the US, the EU, and the UK

Structure of This Report

This report consists of the following three sections:

1. **Structure of Certification**

   This section provides an overview of certification mechanisms for three distinct targets: products, management systems, and operators.

2. **Comparative Analysis of Certification Frameworks Across Jurisdictions**

   Focusing on aspects such as type approval processes and risk-based testing procedures for AVs and MDs, this section examines the certification frameworks in different jurisdictions, highlighting their similarities and differences.

3. **Key Findings and Challenges in AI Certification**

   Based on the analysis in Section **2**, this section identifies common aspects of AI system certification frameworks at present and explores key issues that require further discussion.

1. Structure of Certification

(1) Conventional Certification Frameworks

When certifying a product or system, the certification framework can be categorized into three levels:

(i) Product Certification

Product certification involves evaluating a product itself to determine whether it meets the technical specifications and performance standards set by regulatory authorities.

- Examples:
    - In the case of conventional automobiles, certification (such as type approval) covers compliance with safety standards such as crash tests, emission regulations, and braking performance.
    - In the case of MDs, certification applies to products such as thermometers and infusion pumps, ensuring that thermometers accurately measure body temperature, infusion pumps deliver medication in the correct dosage, and that they comply with safety regulations such as the FDA's 510(k) requirements in the US.

(ii) Management System Certification

Management system certification evaluates an organization's management processes and structures, including risk management, quality assurance, and continuous improvement processes.

- Examples:
    - In the automotive industry, makers obtain certification for compliance with quality management standards such as ISO 9001 and IATF 16949, ensuring that they maintain effective processes for the design, testing, and manufacturing of safe and reliable vehicles.
    - In the medical sector, ISO 13485 serves a similar function for quality management in the manufacturing of MDs.

(iii) Operator Certification

Operator certification ensures that individuals operating or handling a system possess the necessary qualifications and skills to use the technology safely and effectively. This is commonly referred to as "licensure", depending on the industry.

- Examples:

- In the case of conventional automobiles, operator certification takes the form of a driver's license, which verifies that a human driver possesses the skills and knowledge required to operate a vehicle safely.
- In the medical sector, qualifications such as medical licenses or radiologic technologist certifications are required to operate medical equipment such as ventilators and X-ray machines.

(2) Challenges in Certifying AI

Applying the above conventional certification frameworks to AI systems presents several challenges:

- **Challenges and Limitations of Product and Management System Certification for AI Systems**

  The characteristics of AI systems—algorithmic unpredictability, interaction with external environments, and the complexity of system components—make conventional product certify-cation approaches difficult, because product safety standards have relied on specific and detailed technical specifications.

  However, due to the nature of AI systems, establishing fixed, verifiable technical benchmarks is challenging. As a result, there has been a shift towards management system certification, which focuses on evaluating the processes and systems that manufacturers use to ensure ongoing safety and reliability. However, management certification also has its limitations. While it guarantees that manufacturers maintain strong safety and quality processes, it does not immediately ensure the operational safety and real-time reliability of AI systems.

  This real-time assurance is particularly critical for AI systems, which continuously evolve and adapt based on training data or input data. Conventional management certification may not be sufficient to address unforeseen risks and unexpected behaviors that emerge after deployment.

- **Automation of Operators**

  Furthermore, since AI replaces the role of human operators, a key challenge is determining what kind of certification framework should be implemented for its functions.

  In conventional systems, operational safety and reliability depended on human users, such as drivers and doctors. However, with AI-driven automation, some or all of these functions are now performed by the system itself. In this context, the "operator" is no longer the end user but rather the organization that manages the automated system—such as an automobile manufacturer or a medical device producer.

  As a result of this shift, new questions arise: To what extent should these new "operators" be responsible for monitoring AI systems; and how can this responsibility be effectively enforced and assessed?

With these challenges in mind, the next section provides an overview of the legal frameworks established in different jurisdictions.

2. Comparative Analysis of Certification Frameworks Across Jurisdictions

In this section, we conduct a comparative analysis of AI certification frameworks in the regulations governing AVs and MDs across different jurisdictions, including Japan, the US, the EU, and the UK.

For this analysis, we examined regulatory frameworks that define various requirements related to the introduction of AI-enabled products to the market, post-market oversight, and compliance obligations. Based on these findings, we categorized the regulatory frameworks into three levels: product level, management system level, and operator[3] level. By comparing the systems in each jurisdiction across these levels, we identify both commonalities and differences in their regulatory approaches.

(1) Autonomous Vehicles

(i) Japan

a. Product Level

In Japan, the type approval system is implemented under the Act on Vehicles for Road Transportation (AVRT) to streamline the national inspection process for mass-produced vehicles that conform to the same standards while ensuring that each newly introduced vehicle meets the Safety Standards of the Road Transportation Vehicles (Safety Standards).[4] Specifically, if a vehicle manufacturer receives type approval from the Minister of Land, Infrastructure, Transport and Tourism (MLIT) for a vehicle it intends to sell, the manufacturer is required to conduct a completion inspection for each individual vehicle to confirm compliance with the Safety Standards before it can be sold. Upon verification of compliance, the manufacturer must issue a completion inspection certificate for that vehicle.

As part of these standards, the "autonomous operation system" is explicitly designated as a regulated device that must conform to the Safety Standards. This system is defined as a device that fully replaces the cognitive, predictive, judgmental, and operational abilities of the human driver when used under the conditions specified by MLIT, known as the Operating Design Domain (ODD).[5] The details of these safety standards are stipulated in the "Public Notice for Details", which provides specific regulations supplementing the Safety Standards. However, these regulations remain abstract. For instance, the autonomous operation system must: not interfere with the safety of other road users

[3] In this report, the term "operator" is broadly used to refer to individuals or entities that utilize AVs or MDs. For AVs, this includes "drivers" in the case of Level 3 AVs, whereas for Level 4 and above, it encompasses "operating entities" that conduct business using such vehicles.
[4] AVRT Art. 75.
[5] AVRT Art. 41 (2).

during operation and ensure the safety of passengers; enable the vehicle to stop when there is a risk of system malfunction; and be designed with redundancy to prevent critical failures.[6]

Additionally, for conducting public road testing, a road use permit is required under the Road Traffic Act.[7] However, the standards for obtaining this permit are less stringent compared to those required for type approval.[8]

b. Management Level

To obtain type approval, applicants (such as vehicle manufacturers) must submit not only proof of compliance with the Safety Standards but also supporting documents related to: (i) quality control systems; (ii) completion inspection procedures; and (iii) corporate organization and implementation guidelines for inspecting vehicle components, including autonomous operation systems. These documents are subject to review as part of the approval process.[9] However, the requirements specified by law remain highly abstract, and there are no clear regulations defining the specific organizational structures or procedures that must be established for compliance.[10]

c. Operator Level

For Level 3 AVs, a driver's license is required, and the licensed party is the user-driver. In contrast, a 2022 legal revision established a framework allowing certain Level 4 AVs—where a user-driver is not required—to be legally operated. This framework introduced a certification system for operators who put AVs into operational use, even when they are not user-drivers. The purpose of this system is to ensure that existing road safety rules—which may be difficult to comply with solely through an autonomous driving system—continue to be enforced through human oversight. Operators are therefore required to implement compliance measures, such as appointing supervisors to monitor adherence to traffic regulations.

Under the 2022 amendments, the Road Traffic Act (JRTA) established a permit system for "specified autonomous operation."[11] The key provisions include: (i) Entities intending to conduct "specified autonomous operation" must obtain a permit from the prefectural public safety commission with jurisdiction over the area where the operation will take place. (ii) Permit holders ("specified autonomous operation implementers") are required to appoint a "specified autonomous operation supervisor" to monitor system operation

[6] See, Public Notice for Details, Art. 72-2
[7] Road Traffic Act, Art 77.
[8] See, National Police Agency, "Standards for Road Use Permit for Public Road Testing of Autonomous Driving" (September 2024), and Ministry of Land, Infrastructure, Transport and Tourism, "Guidelines for Approval of Standards Relaxation for Vehicles Equipped with Remote Autonomous Driving Systems"
[9] Type Designation Regulations for Motor Vehicles, Art. 3 (2)(iv)-(vi). (In addition, if the applicant has obtained ISO 9001 certification for its quality management system, it is sufficient to attach a document proving this.)
[10] The Notification on the Implementation Guidelines for Vehicle Type Certification (MLIT, Road Transport Bureau, No. 1252, dated November 12, 1998) provides some level of specificity, such as requiring an outline of the inspection process and a diagram of the inspection line. However, regarding organizational structures, the notification only states that "the department in charge of the work (…) should be clearly stated," without specifying further details.
[11] JRTA, Art. 75-12 and following.

and ensure compliance with the designated operational plan. (iii) The specified autonomous operation supervisor must not only oversee the system's operation but also take necessary measures in the event of a traffic accident. Furthermore, amendments to the Road Transportation Act and the Motor Truck Transportation Business Act introduced a requirement that, when conducting passenger or freight transport services using specified autonomous operations, operators must appoint a "specified autonomous operation safety personnel" to handle duties other than driving.[12]

(ii) United States

a. Product Level

In the US, a self-certification system is used. The National Highway Traffic Safety Administration (NHTSA) has established the Federal Motor Vehicle Safety Standards (FMVSS) under the National Traffic and Vehicle Safety Act of 1966, which regulate the safety standards for motor vehicles and related devices.[13] While the FMVSS were slightly revised in March 2022 to consider Level 4 and Level 5 AVs,[14] there are still no specific provisions for autonomous driving devices equivalent to Japan's autonomous operation system.[15]

Due to the absence of federal regulations, individual states have established their own rules. For instance, in California, the Vehicle Code (VHC) contains a dedicated chapter on AVs, titled "Division 16.6 Autonomous Vehicles." This section outlines performance requirements for AVs to operate on public roads. However, as in Japan, these requirements remain abstract, such as mandating that "[t]he autonomous vehicle must have a mechanism to engage and disengage autonomous technology that is easily accessible to the operator[16]." [17, 18]

b. Management Level

Unlike Japan, where type approval requires a prescribed quality management system, neither the FMVSS nor California's VHC mandates such a requirement. However, in practice, it is common for manufacturers in the automotive industry to obtain certification under ISO 9001 (an international standard for quality management systems) and IATF 16949 (a standard specifically for the automotive industry).

---

[12] Ordinance for Enforcement of Road Transportation Act, Art. 51-16-2 (1); Regulations for Safety of Motor Truck Trans-portation Business Act, Art. 3 (1); and so on.
[13] 49 CFR Part 571.
[14] Federal Register Volume 87, Issue 61 (March 30, 2022).
[15] The Federal Automated Vehicle Policy (first issued in September 2016 and revised in September 2017) provides non-binding guidance for autonomous vehicle developers and state governments. It includes safety elements similar to those in Japan's Safety Standards for autonomous operation systems. *See*, https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf
[16] In VEH, the term "operator" refers to "the person who is seated in the driver's seat, or, if there is no person in the driver's seat, causes the autonomous technology to engage" (VEH §38750 (a)(4)).
[17] VEH §38750 (c)(1)(a).
[18] In 2020, the automotive industry issued the UL4600 standard for Level 4 and higher AVs, which was later adopted as an ANSI standard (ANSI/UL4600).

c. Operator Level

In California, there are two permit systems for the operation of AVs: (i) a permit for test-driving AVs on public roads; and (ii) a deployment permit for commercial use of AVs by individuals other than the manufacturer's employees.[19] Unlike Japan, California requires autonomous vehicle operators to secure a certain level of financial responsibility through liability insurance. Additionally, remote monitoring is not mandatory.[20]

(iii) EU

a. Product Level

The regulatory framework for both product-level and management-level certification in the EU follows a dual-layer structure. First, the EU AI Act provides comprehensive governance for AI-specific matters, establishing overarching regulations for AI-related technologies. Second, sector-specific regulations impose additional requirements tailored to individual industries. These sectoral laws not only align with the EU AI Act, but also evolve independently to address AI-related challenges. Regarding the regulation of AVs in the EU, the following key features can be identified:

1. **Two major Regulatory Frameworks:**

   The EU employs two major regulatory structures for AVs: (i) Type-Approval Framework Regulation (TAFR) and (ii) General Safety Regulation (GSR). Under these regulations, AVs and their components must obtain type approval before they can be sold or used, ensuring compliance with all required safety and technical standards.

2. **Mandatory Implementation of Intelligent Systems**[21]:

   The **EU mandates** the integration of **smart technologies** into AV systems to enhance safety. The required features include:

   a. For all road vehicles (i.e. cars, vans, trucks and buses): Intelligent speed assistance, reversing detection with camera or sensors, attention warning.
   b. For cars and vans: Additional features like lane-keeping systems and automated braking.
   c. For buses and trucks: Technologies for better recognition of possible blind spots, warnings to prevent collisions with pedestrians or cyclists and tire For buses and trucks: Technologies for better recognition of possible blind

[19] CCR Title 13, Division 1, Chapter 1, Article 3.7 & 3.8.
[20] However, an unofficial draft amendment for a future regulatory update includes a provision requiring remote monitoring (Potential Draft Regulatory Language, §228.06. Requirements for Remote Drivers and Remote Assistants). *See*, https://www.dmv.ca. gov/ portal/file/article-3-8-express-terms-pdf/ [Last viewed; 23/12/2024]
[21] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_4312

spots, warnings to prevent collisions with pedestrians or cyclists and tire pressure monitoring systems.

3. **Level 3 regulation**:

   For Level 3 AVs operating on highways (where the system replaces the driver), EU regulations align with the United Nations' Level 3 AV standards, ensuring compliance with the latest UN technical regulations[22]. These requirements are primarily technical in nature.

4. **Level 4 regulation**:

   The European Commission has adopted type-approval legislation governing fully autonomous vehicles (Level 4 AVs), including those operating in urban environments. The technical requirements for these vehicles are established through a delegated act[23] and an implementing act[24]. These regulations mandate a comprehensive safety assessment and determine market entry feasibility for fully autonomous vehicles. The requirements include test procedures (crash testing, fuel system integrity, and braking performance), cybersecurity standards, data recording regulations, and safety performance monitoring and accident reporting obligations for manufacturers.

The EU AI Act's **high-risk AI system requirements do not directly apply to AVs.**[25] Instead, existing AV regulations remain in force. However, the EU AI Act mandates that sector-specific AV laws incorporate high-risk AI system requirements. (Annex III, point 5 of the EU AI Act include provisions related to critical infrastructure, such as road traffic.)

Additionally, the **EU has developed a flexible legal framework for AVs** that ensures technological advancements are not restricted while focusing on product-level and management-level regulation. Key regulations include:

- **Regulation (EU) 2019/2144 :** This regulation establishes the type-approval requirements for motor vehicles, including automated items, standards for safety and emissions.
- **Regulation (EU) 2022/1426:** This regulation specifically addresses the type-approval of automated driving systems (ADS) in fully automated vehicles. It is both a specific and high-level document, which generally addresses the technology. It outlines technical requirements and testing procedures.

[22] https://unece.org/media/press/368227
[23] https://eur-lex.europa.eu/legal-content/EN/PIN/?uri=PI_COM:Ares%282022%292077610
[24] https://eur-lex.europa.eu/legal-content/EN/PIN/?uri=PI_COM:Ares%282022%292667391
[25] Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users.

- **Regulation (EU) 2022/2236:** This regulation sets technical requirements for various types of vehicles, including fully automated vehicles, produced in limited series.

b. Management Level

To obtain type approval, vehicle manufacturers must submit proof of compliance with safety regulations alongside supporting documentation related to: (i) Safety and quality management systems, including structured risk assessment and compliance frameworks; (ii) approval and validation procedures, demonstrating that vehicles—particularly those with Automated Driving Systems (ADS)—meet regulatory safety and operational standards; and (iii) corporate governance and oversight mechanisms, detailing how organizations monitor, document, and continuously improve safety-critical processes across vehicle development and production.

Regulatory requirements under **Regulation (EU) 2019/2144**, **Regulation (EU) 2022/1426**, and **Regulation (EU) 2022/2236** establish management-level obligations related to quality control, safety governance, and compliance reporting. However, these requirements remain largely (i) technical, in relation to material product-level safety requirements, and (ii) procedural, rather than prescriptive, leaving flexibility in how manufacturers structure their internal safety and risk management frameworks to reach these technical goals. As a result, organizations must interpret and implement compliance measures based on their operational structure while ensuring alignment with EU type-approval processes.

c. Operator Level

Traditionally, the operator of a vehicle was solely the human driver. However, with the emergence of fully autonomous vehicles, the definition of "operator" has expanded to include manufacturers and entities responsible for the deployment of Autonomous Driving Systems (ADS).

The EU's regulatory approach to fully autonomous vehicles has, thus far, focused primarily on **preventive safety measures** rather than redefining liability structures. Although the EU's regulatory approach primarily emphasizes technical reliability, future frameworks may clarify liability distribution among human operators, manufacturers, and service providers as AV technology advances. For example, operators, including manufacturers, must implement risk management systems, must ensure transparency in identifying potential points of failure ("fault items") [26]; operators must establish appropriate frameworks to mitigate risks associated with such faults; and throughout the type-approval process, operators must disclose safety-related data.

[26] Commission Implementing Regulation (EU) 2022/1426 of 5 August 2022 laying down rules for the application of Regulation (EU) 2019/2144 of the European Parliament and of the Council as regards uniform procedures and technical specifications for the type-approval of the automated driving system (ADS) of fully automated vehicles at Art. 2(7) among others.

(iv) United Kingdom

a. Product Level

The UK enacted the Automated Vehicles Act (AVA) in May 2024 to regulate AVs.[27] This law complements traditional type-approval frameworks and establishes a dual-certification system.

Under this framework, the Secretary of State is delegated the authority to establish certification requirements at the product, management, and operator levels. However, the AVA already includes general guidelines concerning certification. Specifically, the Secretary of State may authorize the operation of road vehicles individually (on a case-by-case basis), or generally (as a broader category of vehicles), provided that the vehicles meet prescribed requirements, including self-driving test criteria.[28] When granting such an authorization, the Secretary of State must identify the specific automated driving features that are deemed to satisfy the self-driving test, and specify how these features meet the relevant test criteria, including[29]:

- whether the self-driving feature is "user-in-charge" or "no-user-in-charge",
- how the feature is engaged and disengaged, and
- the locations and circumstances by reference to which (in the opinion of the Secretary of State) the vehicle satisfies the self-driving test by virtue of the feature.

Furthermore, under the AVA, the Secretary of State is granted the authority not only to establish regulations governing the requirements for authorization[30], but also to amend type approval legislation to ensure its compatibility with automated vehicles [31] . Accordingly, further rulemaking and legislative updates are expected in the future.

b. Management Level

Authorized Self-Driving Entity (ASDE) [32]

Under the AVA, the Secretary of State must impose a requirement that, for a vehicle to be granted authorization, there must be a designated "authorized self-driving entity (ASDE)" responsible for that vehicle.

Furthermore, when imposing this requirement, the Secretary of State must ensure that:

[27] https://www.gov.uk/government/news/self-driving-vehicles-set-to-be-on-roads-by-2026-as-automated-vehicles-act-becomes-law.
[28] Automated Vehicles Act 2024 ("AVA"), Art. 3.
[29] AVA Art. 4.
[30] AVA Art. 5.
[31] Art. 91.
[32] AVA Art. 6.

- The ASDE bears general responsibility for ensuring that the authorized automated vehicle continues to satisfy the self-driving test on an ongoing basis.
- The ASDE meets the following conditions:
  (i) be of good repute;
  (ii) be of good financial standing; and
  (iii) be capable of competently discharging any authorisation requirements imposed on it.

c. Operator Level

No-User-in-Charge Operator[33]

Under the AVA, the Secretary of State has the authority to establish regulations concerning the licensing of no-user-in-charge operators, as well as the requirements for no-user-in-charge journeys and the vehicles used for such operations.

When establishing regulations for licensing no-user-in-charge operators, the AVA imposes requirements similar to those outlined in the management-level framework. Specifically:

- no-user-in-charge operator must bear overall responsibility for detecting and responding to any issues that arise during a no-user-in-charge journey under their supervision.
- no-user-in-charge operator must also meet the following conditions:
  (i) be of good repute;
  (ii) be of good financial standing; and
  (iii) be capable of competently discharging any requirements imposed on it.

Additionally, no-user-in-charge operators are explicitly required to "oversee" no-user-in-charge journeys, as specified in the AVA. While the law establishes this duty, the Secretary of State has not yet enacted specific regulations defining the scope and content of such oversight. As a result, the precise nature of a no-user-in-charge operator's supervisory role remains unclear.

User-in-Charge

The AVA defines a user-in-charge as an individual if[34]:

(i) the vehicle is an authorised automated vehicle with an authorised user-in-charge feature;
(ii) that feature is engaged; and
(iii) the individual is in, and in position to exercise control of, the vehicle, but is not controlling it.

[33] AVA Art. 12.
[34] AVA Art. 46.

A user-in-charge feature refers to a function that enables partial automation for specific segments of a journey, while requiring a human driver to operate the vehicle for the remaining segments.[35]

Furthermore, under the AVA, a user-in-charge is exempt from criminal liability in the following situations:[36]

(i) an offense results from something done by the vehicle while the individual was its user-in-charge; and
(ii) the offence does not also result from the individual's conduct after ceasing to be the user-in-charge falling below the standard that could reasonably be expected of a careful and competent driver in the circumstances.

Automated Passenger Services[37]

The AVA authorizes the appropriate national authority[38] to issue permits for automated passenger services or trials involving automated vehicles. Such permits may be granted for one of two purposes:

- to ensure an exemption from specialized taxi, private hire, and bus regulations[39]; or
- to satisfy the permit requirements for no-user-in-charge operations[40].

When granting a permit, the following details must be explicitly specified.

- the areas in which services may be provided under the permit;
- the vehicles (or descriptions of vehicle) in which services may be provided under the permit;
- the period for which the permit is valid; and
- any conditions subject to which the permit is granted ("permit conditions").

The permit approval process involves multiple authorities, including:

- the national authority
- the licensing authority overseeing taxi and private hire regulations in the relevant geographic area[41]
- the relevant franchising body (for bus operations)[42]

[35] Department for Transport, "Explanatory Notes: Automated Vehicles Act 2024 Chapter 10", p.15.
[36] AVA Art. 47; ibid. p.30.
[37] AVA Art. 82.
[38] This provision allows the Welsh and Scottish Ministers to issue permits for Automated Passenger Services. *See*, Department for Transport, "Explanatory Notes: Automated Vehicles Act 2024 Chapter 10", p.45, https://www.legislation.gov.uk/ukpga/2024/10/pdfs/ukpgaen_20240010_en.pdf
[39] AVA Art. 83
[40] AVA Art. 12
[41] AVA Art. 85, 86.
[42] AVA Art. 86.

Additionally, before granting a permit, the Secretary of State must consult with traffic authorities and emergency services to ensure compliance with broader public safety considerations.[43]

In granting a permit, the appropriate national authority must take into account how automated passenger services should be designed to accommodate the needs of elderly and disabled passengers[44]. Additionally, the authority may include specific requirements related to data privacy management and other relevant safeguards as permit conditions.[45]

(2) Medical Devices

(i) Japan

a. Product Level

In Japan, MDs are subject to a regulatory approval system for marketing[46], under which both the efficacy and safety of the device itself and the quality and manufac-turing management standards of the marketing entity are reviewed. MDs are categorized into three classes—"General Medical Devices," "Controlled Medical Devices," and "Specially-Controlled Medical Devices"[47]—with regulatory requirements varying based on risk level[48]: (i) General Medical Devices, which pose the lowest risk, require only a notification; (ii) Controlled Medical Devices and Specially-Controlled Medical Devices with relatively low risk, for which efficacy and safety can be ensured through established standards, require certification by a registered certification organization; and (iii) Higher-risk MDs require approval from the Minister of Health, Labour and Welfare, with the Pharmaceuticals and Medical Devices Agency (PMDA) conducting the review.

All MDs, including Software as a Medical Device (SaMD), must meet the "Essential Requirements," which outline basic requirements.[49] For SaMD, these requirements specifically mandate: (1) ensuring system reproducibility, reliability, and performance;

[43] AVA Art. 87.
[44] AVA Art. 87.
[45] AVA Art. 88.
[46] "Marketing" is defined as "manufacturing (including cases where manufacturing is outsourced to others, and excluding cases where manufacturing is entrusted by others; (...)) or importing (...) medical devices (...), and then selling, leasing, or providing them respectively, or offering medical device programs (medical devices that are programs; hereinafter the same applies) via telecommunication lines." (PMA, Art. 2(13)). Note that "medical device programs" is equivalent to Software as a Medical Device (SaMD).
[47] General Medical Devices correspond to Class I, Controlled Medical Devices to Class II, and Specially-Controlled Medical Devices to Class III and IV, respectively.
[48] PMA, Art. 23-2-5(1) (Approval); Art. 23-2-23(1) (Certification); and Art. 23-2-12(1) (Notification).
[49] PMA, Art. 41(3) and the circular notice (Ministry of Health, Labour and Welfare, No. 122, dated March 29, 2005). These requirements are based on the basic requirements (GHTF/SG/N41R9:2005, revised to IMDRF/GRRP WG/N47 Final: 2018) established by the Global Harmonization Task Force (GHTF), which was succeeded by the International Medical Device Regulators Forum (IMDRF).

(2) verifying quality and performance based on the latest technology, including considerations for the development lifecycle, risk management, and validation methods for proper operation; and (3) addressing cybersecurity concerns. However, these regulations do not include provisions tailored to the specific characteristics of AI.[50]

Recognizing the emergence of continuously evolving technologies such as AI, the 2019 revision of the Act on Securing Quality, Efficacy, and Safety of Products Including Pharmaceuticals and Medical Devices (PMA) introduced the Improvement Design within Approval for Timely Evaluation and Notice (IDATEN) system.[51] This system enables flexible updates to approval details based on post-marketing performance changes, thus incorporating AI-related considerations into Japan's overall regulatory framework for MD marketing approval.

b. Management Level

To obtain approval for marketing MDs, compliance with the following regulatory standards is required: (i) The QMS Ordinance (relating to standards for quality management of manufacturing)[52]; (ii) The QMS System Ordinance (relating to standards for the quality management system)[53]; and (iii) The GVP Ordinance (relating to standards for post-market safety management)[54].

The QMS Ordinance, issued by the Ministry of Health, Labour and Welfare, specifies standards for manufacturing and quality management of MDs. To ensure international consistency, it aligns with ISO 13485, the global standard for quality management systems in the medical device industry.

The QMS System Ordinance sets forth requirements for manufacturers and distributors to comply with the QMS Ordinance. These include:

- Establishing and effectively operating quality management and oversight systems
- Appropriately managing and storing documents and records
- Deploying personnel such as the overall manufacturing and sales manager and oversight personnel to ensure compliance with the QMS Ordinance

The GVP Ordinance outlines standards for ensuring the safety of marketed MDs. It requires manufacturers to:

- Collect and analyze safety management information related to quality, efficacy, and safety

[50] Some MDs have approval criteria specified in circular notices, but no approval criteria currently exist for MDs that use AI. However, evaluation indicators for medical imaging diagnostic support systems using AI were announced on May 23, 2019, by a research group established by the Ministry of Health, Labour and Welfare in 2005.
[51] PMA, Art. 23-2-10-2.
[52] PMA, Art. 23-2-15(1).
[53] PMA, Art. 23-2-2(1)(i).
[54] PMA, Art. 23-2-2(1)(ii).

- Take necessary safety measures, such as providing information to medical professionals

These ordinances provide general requirements for manufacturing management, quality control, and organizational systems for MDs and do not specifically address MDs that utilize AI.

c. Operator Level

Unlike AVs, current MDs incorporating AI (such as diagnostic imaging support systems) are positioned as tools that assist doctors in their diagnoses. Consequently, when these devices are used in "medical practice," the user must hold a medical practitioner's license.[55] However, no specific discussions or regulations focusing on operator-level requirements for MDs incorporating AI have been identified.[56]

(ii) United States

a. Product Level

In the US, MDs are classified similarly to those in Japan, ranging from Class I (low risk) to Class III (high risk). Class II devices (e.g., infusion pumps) and Class III devices (e.g., pacemakers) require approval from the Food and Drug Administration (FDA). The primary approval process for Class II devices is the 510(k), in which a device is evaluated for "substantial equivalence" to a previously marketed device.[57] However, for devices without a predicate but with a low degree of risk, the De Novo classification process allows for approval based on evidence demonstrating safety and effectiveness in relation to the intended use.[58] For Class III devices, the Premarket Approval (PMA) process applies,[59] which imposes stricter requirements than 510(k) for evidence supporting safety and effectiveness.[60]

Regarding Software as a Medical Device (SaMD), the 21st Century Cures Act of 2016 grants the FDA authority to determine whether certain software should be regulated. Software frequently employing AI, such as those used for processing medical images, is classified as a MD and subject to regulatory oversight.[61]

---

[55] Medical Practitioner's Act, Art. 17.
[56] Furthermore, even when a program using AI is employed for diagnostic or therapeutic support, the diagnosis and treatment are performed by a doctor. According to a circular notice by the Ministry of Health, Labour and Welfare (Health Policy Bureau, No. 1219-1, dated December 19, 2018), this is understood to constitute "medical practice" under the Medical Practitioner's Act, Art. 17.
[57] FDCA510(k)(21USC360(k)), 21CFR807.81(a), 21CFR807.100
[58] FDCA513(f)(2)(21USC360c(f)(2))
[59] FDCA515(21USC360e)
[60] FDCA515(c)(1)(21USC360e(c)(1)), 21CFR814.20
[61] FDCA520(o)(1)(A)-(E)(21USC360j(o)(1)(A)-(E)), FDCA201(h)(1)(21USC321(h)(1))

The FDA has also established "recognized consensus standards" to evaluate MD performance depending on device type.[62] However, no AI-specific standards have been identified in this context.

Recognizing that the performance of AI-enabled MDs may evolve post-market, the Predetermined Change Control Plan (PCCP) system was introduced in 2022. Similar to Japan's IDATEN system, this framework allows for pre-approved modification plans, so that functional changes made after initial approval do not require an additional review process.[63]

b. Management Level

For any of the approval processes mentioned in section *a*, compliance with the Quality System Regulation (QSR) is mandatory, similar to Japan. Previously, the QSR contained requirements differing from ISO 13485:2016, an international quality management standard for MDs. However, a 2024 revision incorporated ISO 13485:2016 requirements into the QSR, with implementation scheduled for February 2026.[64]

c. Operator Level

In the US, AI-enabled MDs, such as diagnostic imaging support systems, are currently positioned as tools assisting doctors in medical practice. Performing medical practice requires a medical license, and specialized procedures necessitate a specialist medical license. Regulatory approval and licensing requirements fall under the jurisdiction of individual states. As in Japan, no specific discussions or regulations have been identified regarding operator-level regulations focused on the use of AI-enabled MDs.

(iii) EU

a. Product Level

The EU employs a multi-layered regulatory approach at both the product and management levels, similar to its framework for automated vehicles. Specifically, regulation is divided into (i) medical device-specific regulations and (ii) general AI-related regulations under the EU AI Act.

---

[62] FDCA514(c)(21USC360d(c))

[63] FDCA515C(21USC360-e). In 2023, a draft guidance on PCCP for AI-enabled MDs was published: "Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence/Machine Learning (AI/ML)-Enabled Device Software Functions." This document outlines recommended elements for inclusion in such plans, including data management (e.g., training and learning data), relearning methods, performance evaluation methods, and update procedures. *See*, https://www.fda.gov/regulatory-information/search-fda-guidance-documents/marketing-submission-recommendations-predetermined-change-control-plan-artificial-intelligence

[64] https://www.fda.gov/medical-devices/quality-system-qs-regulationmedical-device-current-good-manufacturing-practices-cgmp/quality-management-system-regulation-final-rule-amending-quality-system-regulation-frequently-asked

Regarding (i), as in Japan and the US, MDs in the EU are regulated according to their risk classification under the Medical Device Regulation (MDR). Specific compliance requirements are established for each risk class under the MDR, and MDs classified as Class IIa or higher must undergo a conformity assessment by a third-party Notified Body before entering the market

Manufacturers are also subject to post-market obligations concerning product safety.[65] Specifically, as part of their quality management system, manufacturers must conduct post-market clinical follow-up (PMCF) to implement preventive or corrective measures. They are also required to monitor device performance, update technical documentation, and maintain a post-market surveillance system. This system must ensure compliance through a risk management framework aligned with clinical evaluation, under the oversight of qualified personnel. The system must also be proportionate to the risk classification and type of the medical device, ensuring continuous safety and compliance. Collection of clinical data is mandatory. Additionally, manufacturers of high-risk MDs must prepare periodic safety update reports (PSUR), which analyze data obtained through post-market surveillance.[66]

Regarding (ii), the EU AI Act includes provisions relevant to healthcare in Annex III under "Access to and enjoyment of essential private services and essential public services and benefits." The relevant AI systems include:

a. Public Authority Assistance: AI systems used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for essential public assistance benefits and services, including healthcare services, as well as to grant, reduce, revoke, or reclaim such benefits and services

b. Insurance Risk Assessment: AI systems used for risk assessment and pricing in relation to natural persons in the case of life and health insurance

c. Emergency Response Management: AI systems used for evaluating and prioritizing emergency calls, dispatching emergency services (including police, firefighters, and medical aid), and triaging emergency healthcare patients

If a medical device falls under any of the above categories, it will be subject to additional high-risk AI obligations under the EU AI Act. However, the AI Act does not replace or invalidate existing medical device regulatory frameworks but rather complements them.

b. Management Level

In the EU, the governance of AI systems in medical devices at the management level is structured through specific provisions in the Medical Device Regulation (MDR) and the EU

[65] MDR at Preamble, at 20, 32-34, 48. Art. 10 (9)(i); (10); Art. 83; Art. 92.
[66] MDR at Art. 86.

AI Act. These regulations establish responsibilities and obligations to ensure compliance and uphold safety and efficacy standards. Key among the governing documents are the specific direction provided by the MDR and In Vitro Diagnostic Regulation (IVDR), which focus on building institutional capacity through creating an office responsible for regulatory compliance; alongside the general requirements for high-risk systems of the EU AI Act.

1. Medical Device Regulation (MDR)

The MDR mandates that manufacturers and authorized representatives appoint a Person Responsible for Regulatory Compliance (PRRC). The PRRC is responsible for ensuring quality management requirements functionality including regulatory standards being met for relevant medical devices, that technical documentation and EU declarations of conformity are maintained, that post-market surveillance obligations are complied with, and that incident reporting obligations are fulfilled.[67]

2. AI Act

The AI Act through its introduction of risk-based categorization of AI systems, provides a structure by which high-risk AI systems—such as those used in medical devices—are subject to management compliance requirements. Providers of high-risk AI medical devices must implement a quality management system, ensure technical documentation is maintained, conduct conformity assessments before placing systems on the market, and establish post-market monitoring to ensure ongoing compliance and safety.[68]

c. Operator Level

In the EU, medical device operators are typically medical professionals, with responsibility shared between medical professionals and manufacturers.

(iv) United Kingdom

The UK is currently in a transition phase, moving away from the EU's regulatory framework for MDs. Previously, the UK operated under the Medical Devices Regulations 2002, which were based on EU directives and included the CE marking system for product certification. However, in 2023, the UK introduced its independent framework, the UK Medical Device Regulations 2023, establishing a new regulatory system, including provisions for AI-enabled MDs. This transition is occurring gradually, with EU-based certification systems being phased out by 2030.

Key features of the current UK regulatory framework include:

1. Transition from EU Regulation:

[67] Regulation (EU) 2017/745; Regulation (EU) 2017/746, ("MDR" & "IVDR") Art. 15.
[68] EU AI Act Arts. 16-19, 43, 49; Chapter IX, Sections 1, 2.

The CE marking will be accepted until 2030,[69] after which it will be replaced by the UKCA (UK Conformity Assessed) marking, which represents the UK's independent conformity and compliance evaluation system.

Additionally, future UK regulations aim to align the core requirements for MDs more closely with EU standards. This includes cybersecurity requirements for software as a medical device, including AI-based MDs.[70]

2. Risk-Based Certification System:

The UK's medical device classification system generally aligns with the EU's classification framework:

- "Group A device" corresponds to EU Class I medical devices, Class IIa medical devices, and Class IIb medical devices that are neither implantable nor long-term invasive.
- "Group B device" corresponds to Class IIb medical devices that are implantable or long-term invasive, Class III medical devices, and active implantable medical devices.

3. Institutional Structure & Software Group:

The UK has established specialized task forces to develop regulations specifically for AI-enabled MDs, as part of its ongoing regulatory development efforts. [71]

4. International Coordination with the US and Canada:

The UK has announced (a) several collaborative plans with the US and Canada and (b) updates to legacy regulations to accommodate AI-enabled MDs.

(a) Collaborative Plans with the US and Canada:

i. Development of 10 principles,[72] including life cycle considerations and transparency, in coordination with the US Food and Drug Administration (FDA) and Health Canada (HC).

[69] Medicines & Healthcare products Regulatory Agency, Standard: Implementation of the future regulations (https://www.gov.uk/government/publications/implementation-of-the-future-regulation-of-medical-devices/implementation-of-the-future-regulations); Medicines & Healthcare products Regulatory Agency, Guidance: Regulating medical devices in the UK (https://www.gov.uk/guidance/regulating-medical-devices-in-the-uk)
[70] Medicines & Healthcare products Regulatory Agency, Standard: Implementation of the future regulations (https://www.gov.uk/government/publications/implementation-of-the-future-regulation-of-medical-devices/implementation-of-the-future-regulations)
[71] Medicines & Healthcare products Regulatory Agency, Guidance: Software and artificial intelligence (AI) as a medical device (https://www.gov.uk/government/publications/software-and-artificial-intelligence-ai-as-a-medical-device/software-and-artificial-intelligence-ai-as-a-medical-device)
[72] Medicines & Healthcare products Regulatory Agency, Guidance: Good Machine Learning Practice for Medical Device Development: Guiding Principles (https://www.gov.uk/government/publications/good-machine-learning-practice-for-medical-device-development-guiding-principles/good-machine-learning-practice-for-medical-device-development-guiding-principles)

ii. Joint publication of Predetermined Change Control Plans (PCCP) for medical devices incorporating large language models (LLMs) alongside the US FDA and HC.[73]

iii. Establishment of guidelines for stand-alone software as a medical device, including applications classified into four categories:

(i) symptom checkers

(ii) clinical calculators

(iii) "drives or influences the use of a device",

(iv) field safety warnings and end of life notifications[74]

(b) Pre-market requirements will be updated to accommodate AI-enabled MDs,[75] with a focus on ensuring safety, effectiveness, and quality before market entry. These requirements will be proportionate to the risk posed by the device and will reference ISO standards (including IEC 62304:2006).[76]

5. Build-up Phase:

Future core regulation is expected to come out sometime in 2025.[77]

---

[73] https://assets.publishing.service.gov.uk/media/6537be725e47a500149898dc/Predetermined_Change_Control_Plans_-_Guiding_Principles.pdf

[74] Medicines & Healthcare products Regulatory Agency, Guidance: Medical device stand-alone software including apps (including IVDMDs)(https://assets.publishing.service.gov.uk/media/64a7d22d7a4c230013bba33c/Medical_device_stand-alone_software_including_apps__including_IVDMDs_.pdf)

[75] Medicines & Healthcare products Regulatory Agency, Guidance: Software and AI as a Medical Device Change Programme – Roadmap, WP3 Premarket requirements (https://www.gov.uk/government/publications/software-and-ai-as-a-medical-device-change-programme/software-and-ai-as-a-medical-device-change-programme-roadmap#wp-3-premarket-requirements)

[76] https://www.iso.org/standard/38421.html

[77] Medicines & Healthcare products Regulatory Agency, Roadmap towards the future regulatory framework for medical devices(9th January 2024) (https://web.archive.org/web/20240221112716/https://assets.publishing.service.gov.uk/media/659d3539aaae22001356dc3c/Roadmap_towards_the_future_regulatory_framework_for_medical_devices__Jan_24.pdf)

3. Key Findings and Challenges in AI Certification

(1) Key Findings from Comparative Analysis

The commonalities and differences in regulatory frameworks for autonomous vehicles (AVs) and medical devices (MDs), based on the analysis in Section 2, are summarized as follows:

(i) Autonomous Vehicles

- **Commonalities:**
  - **Mandatory regulatory approval** : Regulatory approval is required for both test driving and market introduction of AVs.
  - **Relaxed requirements for test driving:** Regulatory standards for autonomous vehicle testing phases are relaxed.

- **Differences:**
  - **Requirement for type approval:** Japan, the EU, and the UK require type approval by public authorities, whereas self-certification is permitted in the US.
  - **Scope of type approval:** In the US, the focus is primarily on vehicle hardware and software, while in Japan, the EU, and the UK, management systems are also included in the certification scope.
  - **Role of operators:** Japan, the EU, and the UK legally require human supervision, while such supervision is not currently mandated in the US (California).

(ii) Medical Devices

- **Commonalities:**
  - **Risk-based certification:** Certification systems are implemented according to the risk level of MDs.
  - **Positioning of AI-enabled MDs:** AI-enabled MDs are currently positioned as tools that support medical professionals in performing medical procedures.

- **Differences:**
  - **Comprehensive AI regulation in the EU**: In the EU, AI-specific regulations under the AI Act supplement existing medical device regulations, imposing additional obligations on AI-enabled MDs, while no such comprehensive AI-specific regulations exist in other jurisdictions.
  - **Post-market approval flexibility in Japan and the US:** Japan and the US have implemented systems allowing for flexible modification of approval conditions or exemption from additional

approval requirements for MDs, including AI-enabled devices, that undergo continuous performance changes after market entry.

(2) Future Challenges

Beyond AVs and MDs, AI systems replacing conventionally human-executed high-risk activities are expected to expand rapidly. Accordingly, the demand for certification of such AI systems is increasing. Future challenges include the following:

(i) Institutional Framework for AI Certification

a. Scope of Certification Systems

Q1 How can the integration of cross-sectoral and sector-specific certification systems effectively ensure trust in AI systems?

- ISO/IEC 42001 exists as an international standard for AI management systems. However, its scope is limited to management systems and does not extend to the certification of specific AI products or services.
- Beyond sectors with well-established certification frameworks, such as automotive and medical devices, are there emerging industries or service domains where the increasing integration of AI necessitates the development of new certification schemes?

b. Mandatory Certification Requirements under Hard Law

Q2: What areas should require mandatory certification under hard law?

- In fields where certification is already mandatory under existing laws (e.g., AVs, MDs), certification of AI products should also be required as a general rule. However, the scope and methods of certification need further examination (see (ii) below).
- Should additional areas require mandatory certification?
    - The EU AI Act specifies high-risk AI applications in Annex III and mandates conformity assessments.

c. Ensuring Interoperability through International Standards

Q3: What are the challenges in making certification systems interoperable across jurisdictions?

- Particularly, how should differences in requirements such as the necessity of human supervision be addressed across different countries?

(ii) Certification Methods

a. Scope of Certification

Q4: What should be the target of AI certification?

- Conventional product certification methods may not be fully applicable due to several reasons, such as AI's black-box nature and lack of explainability.
- Conversely, certifying management systems or operators does not directly assess the risks of products and services, limiting effectiveness.
- If Joint-Certification approach[78] is adopted, how should it be structured?

b. Certification Standards

Q5: How should certification standards for AI products and services be established?

- The complexity of AI algorithms makes direct trust assessment challenging, unlike traditional waterfall system models.
- If performance-based certification (e.g., accident rate per mileage, misdiagnosis rate per diagnosis) is implemented, can consensus on testing methods be reached?
- If the certification scope includes multiple elements, how should each element be assessed?
- Is it feasible and appropriate to decompose certification elements (e.g., data governance, cybersecurity, algorithm performance, monitoring systems) for individual assessment?
- If Joint-Certification is adopted, what should be the final assessment criteria?

c. Timing of Certification

Q6: At what stage should AI products and services be certified?

- Given continuous updates to AI environments and algorithms post-market, and the rapid pace of technological progress, to what extent should pre-market certification be rigorous?
- How should post-market monitoring be conducted, and who should be responsible for ongoing safety verification?

[78] A joint-certification model layers processes to manage and govern a particular capability area within an organization (e.g., privacy) with the products that capability applies to (e.g., cloud computing offerings). The model relies on applying an ISO/IEC standard for management systems (governance and oversight) with a standard applying to products/services to deliver the flexibility needed. *See* EY and Microsoft, "A Joint Certification Approach for Digital Services and Regulatory Compliance" (2022)

(iii) Certification Bodies

a. Minimum Requirements for Certification Bodies

Q7: What are the minimum requirements for certification bodies, considering the need for high expertise?

b. Involvement of Experts in the Certification Process

Q8: What types of experts should be involved in the certification process?

(iv) Relationship Between Certification and Liability Regimes

Q9: In cases where accidents occur under a certification system, how should civil, criminal, and administrative liability be structured?

Scenario 1: The operator obtained certification and continued operations in compliance with certification conditions.

Scenario 2: The operator obtained certification but failed to comply with certification conditions post-approval.

Scenario 3: The operator did not obtain certification.

On February 4, 2025, the Japanese government's AI Policy Study Group released its interim report, and on February 28, 2025, the Cabinet approved the Bill on the Promotion of Research, Development, and Utilization of AI-Related Technologies. A common feature of these policies is their strong support for AI implementation by private enterprises while entrusting the assurance of AI reliability to voluntary initiatives by businesses. This underscores the growing importance of private-sector-led AI certification mechanisms.

This report provides a summary of the current state of domestic and international regulatory frameworks. A key takeaway from this analysis is that, as of now, AI certification mechanisms remain in the early stages of development across all sectors. The authors hope that the findings and discussions presented in this report will contribute to the advancement of future debates on AI certification systems both domestically and internationally.

Appendix 1:
Preliminary Survey on Legal Certification Systems across Jurisdictions

Note: This preliminary survey provides a general overview of legislative trends in various countries as of August 2024 based on desktop research. It is a survey focused solely on the existence of legal regulations and does not guarantee the accuracy or currency of specific laws.

1. Summary of Survey

- In all surveyed countries, regulatory approval systems for AI systems exist in the fields of medical devices and automobiles.
    - However, this is primarily because certification systems for vehicles and medical devices existed prior to AI implementation, and these systems have subsequently been updated to accommodate AI.
    - Under the EU AI Act, if AI is used as a component of a product where third-party certification is already required under existing EU law, the system is classified as a high-risk AI system, and additional obligations under the AI Act are imposed alongside existing regulatory requirements.[1]

- In contrast, in many countries, AI systems used in the financial, legal, and labor sectors do not have certification systems specifically for AI itself.
    - In these sectors, regulation has conventionally focused on licensing the entities operating such systems, with the assumption that these entities are responsible for ensuring compliance and proper use of AI.

[1] AI Act Annex I. Specifically, it includes: (1) the Machinery Directive, (2) the Toy Safety Directive, (3) the Recreational Craft Directive, (4) the Lift Directive, (5) the ATEX Directive (Equipment for Explosive Atmospheres), (6) the Radio Equipment Directive, (7) the Pressure Equipment Directive, (8) the Cableway Regulation, (9) the Personal Protective Equipment Regulation, (10) the Gas Appliances Regulation, (11) the Medical Devices Regulation, (12) the In Vitro Diagnostic Medical Devices Regulation, (13) the Civil Aviation Safety Regulation, (14) the Regulation on Two-, Three-, and Four-Wheeled Vehicles, (15) the Agricultural and Forestry Vehicles Regulation, (16) the Marine Equipment Directive, (17) the Directive on the Interoperability of the Rail System, (18) the Regulation on Motor Vehicles and Their Components, (19) the Regulation on the Type Approval of Motor Vehicles, and (20) the Regulation on Common Rules in Civil Aviation Safety.

- The EU AI Act, however, mandates certification for high-risk AI systems in addition to existing licensing requirements for operators.

- Several countries and regions are considering special regulations for advanced AI models (e.g., general-purpose AI and frontier AI).
  - The EU and China have already enacted such legal frameworks.
  - Japan and the UK have considered regulatory frameworks but have not enacted specific legislation yet. In the US (California), a law mandating transparency in training data has been enacted. However, the Safe and Secure Innovation for Frontier Artificial Intelligence Act (SB1047) (California AI Safety Act), which aimed to regulate large-scale foundational models, was vetoed by the state governor and subsequently failed to pass.

2. Survey Results

<explanatory notes>

PL: Public licensing is required

TC: Third-party certification is required

SC: self-certification

PR: Public registration is required

UD: Under Official discussion

NA: None

<Categories and possible use cases[2]>

Healthcare: Diagnosis, Symptom prediction, Surgery assistance, Personalized treatment plans

Mobility: Autonomous vehicles, Traffic management, Predictive maintenance, Route optimization

Finance: Fraud detection, Algorithmic trading, Credit scoring, Customer service chatbots

Legal: Document review, Predictive analytics for case outcomes, Contract analysis, Legal research

Generative AI: Content creation, Language translation, Personalized marketing, Code generation

Labor: Workforce management, Skill matching, Employee performance analytics, Predictive hiring

	Healthcare	**Mobility**	**Finance**	**Legal**	**GenAI**	**Labor**	**Other Comments**
Japan	**PL** Act on Securing Quality, Efficacy and Safety of Products Including Pharmaceuticals and Medical Devices	**PL** the Act on Vehicles for Road Transportation, Road Traffic Act	**PL** Installment Sales Act to become the "Certified Comprehensive Credit Purchase Intermediary" (※J1)	**NA**(※J2)	**UD**(※J3)	**NA**	

[2] The following examples are not necessarily covered by regulations in each jurisdiction.

	Healthcare	Mobility	Finance	Legal	GenAI	Labor	Other Comments
EU	**PL** Medical Devices Regulation (MDR), and the In Vitro Diagnostic Medical Devices Regulation (IVDR) **TC/SC** AI Act (High risk AIs include: (i) Public authority assistance, (ii) insurance risk assessment, (iii) Emergency response management)	**PL** Type-Approval Framework Regulation (TAFR) and (2) the General Safety Regulation (GSR) **UD** Autonomous Vehicles (sectorial regulation)	**TC/SC** High risk AIs include: Credit-worthiness.	**TC/SC** High risk AIs include: (i) Judicial and dispute resolution assistance, (ii) Election/public opinion influence	**TC/SC** Systemic Risk: Notification to Commission, and publicly listed	**TC/SC** High risk AIs include: (i) Recruitment and selection, (ii) Workplace decisions	Under the AI Act, High-risk AIs will have to (a) register in a EU database, and (b) perform pre-market Conformity Assessments (CAs). Generally, for AIs classified as high-risk systems: (i) When there's no harmonized standards, then Mandatory TC CA; (ii) where there are harmonized standards, then Mandatory SC CA. General Purpose AIs have their own assessment.

	Healthcare	**Mobility**	**Finance**	**Legal**	**GenAI**	**Labor**	**Other Comments**
US (Federal/other)	Federal: **PL** Federal Food, Drug, and Cosmetic Act (all medical devices are subject to the Federal permission)	Federal: **PL** (※US1) Safely Ensuring Lives Future Deployment and Research In Vehicle Evolution Act (2017) States: **PL/UD** Many states including California, Florida, Arizona etc. introduced State acts.	Federal: **NA** (※US2)	Federal: **NA**	Federal: **NA** California **UD** Safe and Secure Innovation for Frontier Artificial Intelligence Models Act (SB1047) (※ US3)	Federal: **NA** New York City: **TC** for hiring algorithms	Colorado: **NA?** "Consumer Protections in Interactions with Artificial Intelligence Systems" (the Colorado AI Act) (※ US4)
UK	**PL/UD** 英国 Medical Devices Regulations	**PL** Automated Vehicles Act 2024	**NA** The FCA (Financial Conduct	**NA**	**NA (UD?)** On July 17, 2024,	**NA**	The UK Government's March 2023 white paper 'A pro-innovation approach to AI

	Healthcare	Mobility	Finance	Legal	GenAI	Labor	Other Comments
	2002 (Detailed guidance specifically for AIaMD products to b e provided in Spring 2025)	(Authorisation of road vehicles for automated use/ Licensing of operators for vehicle use without user-in-charge/ Permits for automated passenger services)	Authority) addresses a tech-neutral approach (AI Update, 3.2)		it was reported that the new governme nt aims to regulate most powerful AI models		regulation' laid out the framework for current plans to regulate of AI. This would take a non-statutory approach, relying on existing regulators to oversee the use of AI in their areas while following five broad principles: safety, transparency, fairness, accountability, and contestability.
Canada	**PL** Canada's federal Medical Device Regulations (SOR/98-282) under the Food and Drugs Act require pre-market approval (licensing) for	**PL** In 2018 the Motor Vehicle Safety Act was amended to add limited exemptions for AVs meeting certain standards.	**UD** Bill C-27 may be applicable	**UD** Bill C-27 may be applicable	**UD** Bill C-27 may be applicabl e	**UD** Bill C-27 may be applicable	Bill C-27 (the proposed "AI and Data Act") is under parliamentary discussion and would impose obligations (e.g. risk management, assessment) on "high-impact" AI systems. The definition of high-impact AI systems is

	Healthcare	Mobility	Finance	Legal	GenAI	Labor	Other Comments
	software as a medical device (including AI).	Provincial pilot programs govern autonomous vehicle testing; no finalized nationwide AV regulation yet.					not clear but it may cover AI systems impacting access to services or employment, biometric identification and inference, large-scale behavior influence, and critical health and safety.
Singapore	**PL** (※S1) Health Products Act 2007 (as detailed guidelines and guidance, "Regulatory Guidelines for Software Medical Devices – A Life Cycle Approach Revision 2.0"	**PL** (※S2) Road Traffic (Autonomous Motor Vehicles) Rules 2017(as detailed standards, "Technical Reference 68 (2019), which	**NA** (※S3)	**NA** (※S4)	**NA** (※S5)	**NA** (※S6)	

	Healthcare	Mobility	Finance	Legal	GenAI	Labor	Other Comments
	and "Medical Devices Guidances")	was revised in 2021)					
China General registration requirements, and security assessments, for algorithms with (a) public opinion properties or (b) the capacity for social mobilization	**PL** (1) Devices: Depending on risk Classification; (2) Practice: Local laws (i.e. Beijing prohibits use of AI in diagnosis and treatment services w/o supervision)	**PL** (Public Trans.) TC/SC (Private Trans.: Safety guidelines)	**PR** (Must (i) have "investment advisory qualifications", and (ii) "file the main parameters of its artificial intelligence model and the main logic of asset allocation with the financial regulatory authority.	**NA** (encouragement for development in judicial decision-making)	**PR** Registration requirements, and security assessments, for algorithms with (a) public opinion properties or (b) the capacity for social mobilization	**NA** (specific protection in Algorithm Law)	

Note

Japan

J1 (Finance)

・The Installment Sales Act establishes regulatory certification related to "AI-based loan amount calculations." The enforcement regulations of this Act set out the general requirements for AI-enabled systems that are approved for use. However, no general legal regulations (such as certification, accreditation, or registration systems) concerning AI usage in the financial sector have been identified at this time.

・The Financial Data Utilization Association (FDUA), an industry group comprising banks and life and non-life insurance companies, published the "Financial Generative AI Practical Handbook" (May 2024) and the "Guidelines for the Development and Use of Generative AI in Financial Institutions" (August 2024). However, neither document considers AI certification or similar regulatory measures.

J2 (Legal Advice)

・While there are no general AI regulations for legal advice, the Ministry of Justice issued a guideline in August 2023 concerning the use of AI in "contract review" and its relation to Article 72 of the Attorneys Act ("Guidelines on Providing Contract and Related Document Support Services Using AI and the Relationship with Article 72 of the Attorneys Act"). This guideline is currently the only identified regulatory document related to AI in legal advice. There appear to be no significant discussions on introducing further regulations at this time.

J3 (GenAI)

・Discussions are currently underway in the AI Strategy Council of the Cabinet Office regarding generative AI regulations.

United States

US1 (Mobility)

・At the federal level, a key law governing autonomous vehicles is H.R. 3388, the Safely Ensuring Lives Future Deployment and Research in Vehicle Evolution (SELF DRIVE) Act, which was passed on June 9, 2017. The law allows states to enact laws regarding automated vehicles, provided they are identical to federal standards, effectively paving the way for state-level legislation. Moreover, the law requires the Department of Transportation to conduct safety assessments and establish a Highly Automated Advisory Council.

(*See:* https://www.holisticai.com/blog/ai-regulations-for-autonomous-vehicles ;
see also: https://www.jetro.go.jp/biz/areareports/2023/bcdf631c4ffdb352.html,
https://www.jetro.go.jp/biznews/2024/04/65d431a83da79f72.html)

US2 (Finance)

・The Executive Order instructs the Consumer Financial Protection Bureau (CFPB) and the Federal Housing Finance Agency (FHFA) to require the entities they regulate to use AI tools to ensure compliance with federal law, evaluate underwriting models for bias against protected groups, and assess automated collateral valuation and appraisal processes to minimize bias.

・The Executive Order establishes an expectation that regulatory agencies use their authority to protect American consumers from fraud, discrimination, and threats to privacy, as well as to address risks to financial stability. Agencies are also directed to clarify where existing regulations or guidance apply to AI.

・The Executive Order specifically references vendor due diligence (such as that described in the June 2023 Interagency Guidance on Third-Party Relationships: Risk Management, issued by the Federal Reserve Board (FRB), Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC)). It also cites requirements and expectations related to transparency and explainability of AI models, such as the OCC's Handbook on Model Risk Management, which instructs examiners to assess explainability if a bank uses AI models in its risk assessment rating methodology.

(*See*: https://www.skadden.com/insights/publications/2023/12/how-regulators-worldwide-are-addressing-the-adoption-of-ai-in-financial-services)

US3 (GenAI)

・AI developers are required to appoint a senior executive responsible for ensuring compliance, including the enforcement of safety and security protocols, oversight of adherence by employees and contractors working on the target model before training begins, and conducting audits, including third-party audits.

(*See*：https://www.nikkei.com/prime/digital-governance/article/DGXZQOUC241HT0U4A620C2000000)

US4

・This legislation requires AI system developers and deployers to exercise reasonable care to prevent consumers from experiencing discriminatory treatment due to algorithmic decision-making in education, employment, financial services, government services, healthcare, and other fields. Specifically, developers are required to: (i) prepare statements regarding the type of AI system and its governance structure; and (ii) ensure that deployers have access to the necessary information to conduct impact assessments. Deployers are required to: (i) implement risk management policies and programs for AI systems; (ii) complete impact assessments on system operations; (iii) notify consumers of specific details when the system makes decisions affecting them; and (iv) if an AI system makes adverse decisions about consumers, provide—where technically feasible—an opportunity for consumers to challenge the decision through human review.

・Additionally, both developers and deployers must disclose risks to the Attorney General within 90 days if they determine that the system has caused discriminatory outcomes. Notably, the legislation does not include provisions for private rights of action, meaning enforcement authority rests solely with the Attorney General's Office. However, if developers and deployers comply with the specified requirements, they will be presumed to have exercised reasonable care.

(*See*：https://www.jetro.go.jp/biznews/2024/05/f8314d21a2862c13.html; https://www.perkinscoie.com/en/news-insights/states-begin-to-regulate-ai-in-absence-of-federal-legislation.html)

Singapore

S1 (Health Care)

・Under the Health Products Act 2007, a licensing system applies to medical devices, including those utilizing AI. Specific requirements are addressed through guidelines such as the "Regulatory Guidelines for Software Medical Devices – A Life Cycle Approach Revision 2.0" (April 2022) and "Medical Devices Guidance."

S2 (Mobility)

・The evaluation and certification of autonomous vehicles are conducted by the Centre of Excellence for Testing & Research of Autonomous Vehicles (CETRAN) under the Road Traffic Act and, more specifically, the Road Traffic (Autonomous Motor Vehicles) Rules 2017 (RTA 2017). These processes include document review and on-road testing in testbeds.

・The Technical Committee on Automotive supervises the development of Technical Reference 68 (TR 68), a provisional standard for autonomous vehicles. TR 68 was first published in 2019 and revised in 2021. The development of TR 68 was carried out by four working groups composed of representatives from the AV industry, research institutions, higher education institutions, and government agencies. The standard is subject to periodic updates based on industry feedback.

S3 (Finance)

・No certification systems appear to have been established.

・The Monetary Authority of Singapore (MAS) introduced the "Principles to Promote Fairness, Ethics, Accountability, and Transparency (FEAT)" in November 2018 and published a white paper in February 2022 detailing evaluation methods. Additionally, in June 2023, the Veritas Consortium, an industry group led by MAS and comprising 31 companies, released a toolkit to help financial institutions implement these evaluation methods. These measures are considered part of a "soft law" approach.

S4 (Legal Advice)

・No certification systems or legal regulations appear to have been established.

・In late May 2024, the Infocomm Media Development Authority (IMDA) and the Singapore Academy of Law announced plans to jointly develop a new large language model (PLM) for use in legal research. This initiative suggests the potential for future applications of such technologies in the legal advice domain.

(*See*, https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/factsheets/2024/gpt-legal)

S5 (GenAI)

・No certification systems appear to have been established. (The "Model AI Governance Framework for Generative AI," published in late May 2024 by the AI Verify Foundation and IMDA, mentions the need for third-party testing but only in general terms.)

・In June 2023, the Infocomm Media Development Authority (IMDA) and Aicadium (an AI solutions company under Singapore's sovereign wealth fund, Temasek Holdings) published "Generative AI: Implications for Trust and Governance." During the same month, IMDA announced the development of "AI Verify," an AI governance testing framework and software toolkit to verify AI reliability. Simultaneously, the "AI Verify Foundation" was established to promote responsible AI use and meet the needs of global businesses and regulators.

・In late May 2024, the AI Verify Foundation and IMDA released the "Model AI Governance Framework for Generative AI." This new framework was specifically designed for generative AI and builds on earlier frameworks for conventional AI, first published by IMDA and the Personal Data Protection Commission (PDPC) in 2019 (updated to Version 2.0 in 2020).

S6 (Workforce & Labor)

・No legal regulations or discussions specifically concerning AI use in labor-related matters have been identified. General ethical principles, such as those in the "Model AI Governance Framework 2nd Edition" (Jan 2020), highlight the need to consider discriminatory impacts in AI-based decision-making under the "Fairness" section.

Appendix 2:
European Union: Overview of AI Act Requirements for High-Risk AI Systems

MARKET-ACCESS REQUIREMENTS UNDER THE EU AI ACT: HIGH-RISK CLASSIFICATION FOR AUTONOMOUS VEHICLES AND MEDICAL DEVICES

Socol de la Osa, David Uriel

This appendix provides an overview of the general requirements under the EU AI Act, focusing on certain processes needed for market access for AI systems that may impact the critical sectors of (i) healthcare, focusing on medical devices, and (ii) mobility, with a focus on autonomous vehicles.

EU regulation pertaining to market-access on the selected category of AI systems operates within a two-tiered regulatory framework:[1]

1. **General AI governance under the AI Act**, which sets requirements for AI systems based on their risk classification.
2. **Sector-specific regulations**, such as the Medical Device Regulation (MDR)[2] for medical devices and the Type-Approval Framework Regulation (TAFR)[3] for autonomous vehicles.

SCOPE OF THIS APPENDIX

This appendix focuses on the general AI Act requirements for autonomous vehicles (AVs) and medical devices (MDs) as high-risk AI systems (HRAIs), rather than sector-specific regulations. While AI in mobility and healthcare may also fall under industry-specific frameworks, this section highlights the AI Act's overarching compliance obligations and how they apply to AV and MD components classified as high-risk. By detailing these requirements, the appendix complements the main report by clarifying the baseline regulatory expectations for AI systems in high-risk domains.

[1] See discussion supra Sections 2(1)(iii) and 2(2)(iii).
[2] This includes Regulation (EU) 2017/745, OJ L 117, 5.5.2017, p.1-175; Regulation (EU) 2017/746, OJ L 117, 5.5.2017, generally regulating medical devices and in vitro diagnostic medical devices.
[3] This includes Regulation (EU) 2018/858, OJ L 151, 14.6.2018, p. 1–218; Regulation (EU) 2019/2144, OJ L 325, 16.12.2019, p.1-40; Commission Implementing Regulation (EU) 2022/1426, OJ L 221, 26.8.2022, p.1-64; generally regulating type-approval as well as specifically addressing autonomous vehicle items.

Key areas covered include:

- **AI system classification under the AI Act** and its intersection with AVs and MDs.
- **Registration duties** for high-risk AI systems before market entry.
- **Conformity assessment procedures**, outlining when self-assessment is permitted and when third-party evaluations are required.
- **Compliance requirements**, including risk management, human oversight, and technical documentation.

GENERAL REQUIREMENTS AND COMPLIANCE PROCESS FOR HIGH-RISK AI SYSTEMS UNDER THE EU AI ACT

High-risk systems (HRAIs): A system is generally considered a HRAI it poses significant risks to harm an individual's health, safety, or fundamental rights.[4] The selected sectors in the report (AVs and MDs) contain components that may qualify as high-risk AI systems, particularly where they intersect with critical functions in healthcare and mobility. Annex III explicitly designates certain applications—such as road traffic management and insurance risk assessment—as high-risk.

Registration Duties: Before placing a high-risk AI system on the market or into service, providers must register the system in the EU database under European Commission supervision (Arts. 49, 71).

Ex-ante conformity assessments (CAs): Under the EU AI Act, providers of HRAIs are required to conduct ex-ante conformity assessments—a key compliance measure that must be completed prior to market entry, in addition to registration (Chapter III, Section 5).

- *Compliance*: These assessments are a means of demonstrating compliance with the requirements set out throughout the AI Act. Developers of HRAIs must perform CAs before placing the system in the EU market (Art. 43).
- *Who conducts these assessments*: CAs can be conducted either internally by the provider or through a notified third-party entity ("notified body", who shall conduct the assessment of Annex VII), depending on the sector of the AI system, and the presence and usage of harmonized standards (Arts. 40-43; Recitals 78, 123-128, 147).
    - Internal assessment: Providers of high-risk AI systems can generally conduct internal conformity assessments (Annex VI) without the involvement of a notified body. This applies to all high-risk AI systems listed under Annex III, Points 2-8 (which includes applications in healthcare as well as mobility in the context of traffic as critical infrastructure). However, for Annex III, Point 1 (biometric AI systems, where permitted under Union or national law), internal assessment can only be used if harmonized standards (Art. 40) or common specifications (Art. 41) exist and have been fully applied.

[4] See discussion infra Appendix II, Section 1.2 for more specificity on what may qualify as a high-risk AI system. See also Regulation 2024/1689, of the European Parliament and of the Council of 13 June 2024, laying down harmonised rules on artificial intelligence, 2024 O.J. (L 210) 1 ("AI Act") at Art. 6, Recitals 46–63, Annex I, Annex III. Throughout this Appendix, all in-line references to articles, sections, or chapters, pertain to the AI Act unless explicitly stated otherwise.

- Third-party or "notified body": If harmonized standards do not exist, cannot be fully applied, or if common specifications are unavailable, a third-party conformity assessment (Annex VII) is required. This always applies to biometric AI systems (Annex III, Point 1) when harmonized standards or common specifications are not available or have not been fully applied. However, for all other high-risk AI systems (Annex III, Points 2-8), only internal assessment is required, with no obligation to involve a notified body.
- Process Items:
  - Notified bodies: Notified bodies are designated by member states (Art. 28; Chapter III, Section 4)
  - Harmonized standards, common specifications: AI systems that comply with harmonized standards are presumed to conform with the AI Act's legal and technical requirements. The development of these standards is a multi-stakeholder process: The European Commission issues standardization requests, which are then developed in collaboration with European Standardization Organizations (ESOs), expert committees, national authorities, and other stakeholders. Once finalized, these standards become officially recognized through publication in the Official Journal of the European Union (OJEU). If harmonized standards are unavailable, delayed, or fail to adequately address fundamental rights concerns, the European Commission may adopt common specifications through implementing acts, ensuring regulatory clarity in the absence of formalized standards. (Arts. 40, 41; Recital 121).

- *Who has to take the assessments*: Generally, HRAI providers are responsible for conducting conformity assessments before placing their AI systems on the market (Arts. 16, 25). However, there are exceptions where this responsibility shifts to other entities, or under which other entities may be considered providers under the AI Act. For example, manufacturers may be subject to the provider's obligations if AI systems that are safety components of products covered by harmonized legislation (Annex I) is placed on the market or put into service under the manufacturer's name or trademark, whether together with the product or after its initial placement on the market. (Art. 25(3)). Additionally, importers, distributors, or deployers may be considered providers and required to carry out duties with regards to conformity assessments if they introduce an HRAI under their own name or trademark, modify the intended purpose determined by the provider, or make substantial modifications that affect compliance, depending on the role they play along the AI value chain, with obligations varying according to the risk of the AI system (Arts. 23-27; Recitals 83-90).

- *Scope of the conformity assessments, key compliance areas*: conformity assessments (CAs) are required to demonstrate compliance with the obligations set out in Chapter III, Section 2. These assessments evaluate whether a high-risk AI system (HRAI) meets the legal, technical, and procedural requirements necessary for market placement and continued operation. (Art. 43).

  The key areas assessed include:
  - *Risk management system* – Implementation of risk mitigation measures throughout the AI lifecycle (Art. 9).
  - *Data and governance* – Ensuring high-quality datasets, bias mitigation, and traceability (Art. 10).
  - *Technical documentation* – Maintaining detailed records on system design, training processes, and functionality (Art. 11).
  - *Record-keeping* – Logging system performance, decisions, and data processing for accountability (Art. 12).
  - *Transparency and provision of information to users* – Clearly communicating system capabilities, risks, and limitations (Art. 13).
  - *Human oversight* – Establishing human intervention mechanisms where necessary to prevent automation risks (Art. 14).
  - *Accuracy, robustness, and cybersecurity* – Ensuring system reliability, resistance to adversarial attacks, and resilience against errors (Art. 15).
  - *Additional Requirement: Fundamental Rights Impact Assessment (FRIA)* – High-risk AI systems must undergo an FRIA to assess their potential effects on fundamental rights (Art. 27).

- *Validity period*: Notified bodies can extend certificates for periods up to 4-5 years, depending on the categorization of the AI system. Certificates can be suspended or withdrawn when AI systems cease to meet compliance standards (Art. 44).

Key Takeaways:

- *Conformity Assessments (CAs)*: Under the EU AI Act, conformity assessments are mandatory for ensuring accountability in the development and deployment of High-Risk AI Systems (HRAIs).
- *Purpose of CAs*: CAs are used to demonstrate compliance with the specific requirements outlined throughout EU AI Act for AI systems, particularly those listed in Chapter III, Section 2.
- *Timing of CAs*: Developers must complete a conformity assessment before introducing a High-Risk AI System to the market or using it for the first time in the EU.

- *Conducting CAs*: Conformity assessments can be conducted (i) internally, generally by the provider, or (ii) by an external, notified third-party entity (designated by the relevant member state), depending on whether harmonized standards or common specifications exist and are used.

1.2 Sector Analysis:

Under the EU AI Act, an AI system is classified as high risk if it meets the criteria outlined in Article 6, as well as the considerations set forth in Recitals 46–63, and whether or not specific AI systems are covered by EU harmonization legislation listed in Annex I. Broadly speaking, a system is considered high risk if it poses a significant risk of harm to the health, safety, or fundamental rights of natural persons. This includes AI that materially influences decision-making processes in ways that could adversely impact individuals. The classification also accounts for the severity and scale of potential harm, the intended use of the system, and the degree of human oversight in its operation.

Given these criteria, many AI applications in the fields of autonomous mobility and healthcare may fall within the scope of high-risk AI. AI used in autonomous vehicles (AVs)—particularly in safety-critical applications like navigation, collision avoidance, and real-time decision-making—has the potential to directly affect human life and public safety. Similarly, medical devices (MDs) that incorporate AI for diagnostics, treatment recommendations, or risk assessments can significantly impact patient health and clinical outcomes.

Beyond these general criteria, Annex III of the AI Act explicitly designates certain AI systems as high risk, specifying particular applications within the AV and MD domains that warrant heightened regulatory scrutiny. While the AI Act does not replace sector-specific regulations, it imposes additional obligations on certain AI systems within high-risk domains, including those in (i) healthcare and (ii) mobility.

i. Healthcare

Annex III, Point 5(a), (c), (d) classifies AI systems in healthcare as high risk, falling under "Access to and enjoyment of essential private services and essential public services and benefits." AI applications in this category include:

- *Public Authority Assistance*: AI systems used by public authorities or on their behalf to determine eligibility for essential public benefits and services, including healthcare management (e.g., granting, reducing, revoking access).
- *Insurance Risk Assessment*: AI-driven systems used for assessing risk and determining pricing for life and health insurance at the individual level.

- *Emergency Response Management*: AI tools used for evaluating and prioritizing emergency calls, dispatching emergency services (police, firefighters, medical aid), and triaging emergency healthcare patients.

Beyond these explicitly listed applications, AI-driven diagnostics, robotic-assisted surgeries, and predictive analytics in disease prevention also fall under scrutiny, particularly when used in critical decision-making that may significantly impact patient outcomes.

ii. Mobility

While the AI Act does not directly regulate autonomous vehicles (AVs), it imposes high-risk classification on specific AI applications within mobility—particularly those related to road traffic management and public safety. Annex III, Point 2 identifies AI in critical infrastructure (road traffic) as high risk, covering applications in:

- *Traffic Management & Road Safety Systems, Critical Infrastructure*: AI systems that influence essential infrastructure networks are subject to high-risk classification under the AI Act. This may include AI-driven technologies that play a significant role in accident prevention, traffic flow optimization, and public safety enforcement. In particular, AI-powered systems managing road congestion, pedestrian crossings, and traffic regulation could fall within this category, depending on their impact on critical infrastructure operations.

Beyond this, other AI applications in mobility may also fall within the AI Act's high-risk classification, though this remains less explicitly defined in the regulation:

- *AI-Based Driver Assistance & Collision Avoidance*: While fully autonomous vehicles (AVs) remain primarily governed by sector-specific regulations (e.g., TAFR), AI subsystems used for real-time safety-critical decisions—such as lane-keeping assistance, automatic braking, and hazard detection—could be interpreted as high risk under the AI Act if their functions significantly impact public safety or infrastructure integrity. However, the extent to which these systems fall within the AI Act's scope remains subject to regulatory interpretation, future enforcement practices, and how the AI Act interacts with specific sectorial regulation.
- *Public Transportation AI Systems*: AI systems deployed in public transit networks for passenger safety, scheduling, predictive maintenance, and incident response could also be relevant under the AI Act's high-risk framework. Given that public transportation constitutes essential mobility infrastructure, certain AI applications in this space may require compliance with AI Act provisions—particularly where their failure or mismanagement could lead to service disruptions or public safety concerns. However, the precise regulatory treatment of such systems remains

uncertain and will likely depend on how authorities interpret their role within critical infrastructure classifications.

While autonomous driving technologies remain primarily within the jurisdiction of sectoral regulations, the AI Act establishes baseline obligations for safety-critical AI applications that influence road safety and traffic management through the classification of critical infrastructure. The intersection between mobility-specific laws and AI regulations will likely evolve as harmonized standards develop and specific AI-driven AV components face additional scrutiny under both transportation and AI governance frameworks.