1. To what extent has the consultation RIS fully and accurately described the problem to be addressed, including the in-service safety risks? Please provide detailed reasoning for your answer.

The RIS lists a range of issues that may impact the safety of the autonomous vehicle systems but is likely over simplistic and fails to understand , from a technical perspective, the hazards associated with the ongoing operation of complex systems.

Complex system failures are most likely to include:

- Design errors resulting in failure of the Design Assurance process
- Erroneous assumptions made at the design stage.
- Changes in operating conditions assumed at the design stage
- Errors in human behaviour assumptions at the design phase
- Durability failures in hardware components - components not meeting failure probability objectives.

There are a second category of failures that are identified by the RIS but require substantially less complex monitoring. These include issues such as

- damage to system hardware, that can occur at only point not just during servicing and will be identified by Built in Test
- Failure to update software - which can be simple identified by monitoring.
- Road rule breaches - which are crude failures easily identified.

The related issue is that often in complex systems failures can be signalled by safety margins being slowly eroded. As an example if a particular sensor input should initiate braking when an obstacle is within 5 meters of a vehicle, but braking is routinely no commencing prior to 3 meters then this is a hazard, and a failure , even if it does not result in any observable impact to the operation.

Such issue are identified by performance monitoring which is a far more complex process than crude failure logging. Such ‘trend monitoring’ is normally considered a key methodology in complex system safety management.

The random list of failures contained in Figure 7 are not incorrect as such, but they are an oversimplified sub set of complex system failure behaviours that could mislead reviewers of the RIS.

2. **Have we correctly identified the parties with an influence on the in-service safety of automated vehicles and accurately described their role? If you identify additional parties, please explain what their role is.**

3. **Have we accurately assessed each party's influence on the in-service safety of automated vehicles? If not, please provide details.**

ADSE Comment - In paragraph 4.3.1 the ADSE is defined as possibly being parties involved in the entry of the product into the market. It is noted that the ADSE could be a third party entity contracted by any of the listed parties to support the product in the market. For instance it is possible to imagine that small volume manufactures may wish to use a third party safety monitor if they only have a small number of vehicles in the Australian market. It is possible to envisage a third party safety assurance provider having a portfolio of ADS products that they aggregate in order to spread costs.

Proposed Influencing Party	Comment
ADSE	Agreed - although it is noted that the 'safety criteria' is likely to be a wider group of criteria more aligned with the particular failure modes of complex systems.
ADSE Executives Officers	Concept Agreed - rather than the generic 'executive officer' description it may be preferable to use he terminology 'accountable manager' which is a concept used in like systems in rail and aerospace and denotes a specific individual rather than a group, where responsibility can be diluted or confused.
Component (ADS) Manufactures	The Component Manufacture provides a product that is approved by the coordinating entity as it is incorporated into the delivered system. Quality failures etc by component manufactures will have an impact on in service system safety but it is important to understand the relationship between suppliers and prime contractors. Only one single entity can have responsibility for initial design safety assertion and ongoing system safety.
Vehicle Manufacture	There is confusion here between the vehicle manufacture and the entity responsible for the design integrity of the ADS. As long as a manufacture ensures a system has been integrated and installed as per the ADS responsible entity instructions then the vehicle manufacturer may have no responsibility for or influence on ongoing safety
Remote Driver	The remote driver should be considered a subset / function of the ADSE
Fallback Ready User	Agreed - however it remains the responsibility of the ADSE to ensure that the Fallback ready user is sufficiently competent (trained) and maintains suitable ongoing vigilance. How this is achieved is considered a design and operational attribute of the system that must be managed by the ADSE
Repairers	Not Agreed - Repair errors should be identified by either Built in Test or some other form of monitoring that should be the responsibility of the ADSE
Modifiers	Not Agreed - Modification errors should be identified by either Built in Test or some other form of monitoring that should be the responsibility of the ADSE

Proposed Influencing Party	Comment
Registered Owners	Not Agreed - Owner errors or emissions should be identified by either Built in Test or some other form of monitoring that should be the responsibility of the ADSE
Road Managers	Not Agreed - Only the ADSE has access to the design assumptions regarding the operating environment. It is not possible for Road Managers to understand how any given change to the road environment may or may not impact the ADS. The ADS must be able to accommodate or identify environments not covered by the design baseline. The ADSE should be monitoring for failures that result from incompatibility between operating environment and design assumptions regarding the operating environment.
Commercial Operators	Not Agreed - Operator errors or emissions should be identified by either Built in Test or some other form of monitoring that should be the responsibility of the ADSE
Human Drivers	Agreed - Highly limited influence
Passengers	Agreed - Highly limited influence
Other road users	Agreed - Highly limited influence
Vehicle Inspectors	Agreed - Highly limited influence
Dealers	Not agreed - influence is so limited as to be not relevant
Distributors	Not agreed - influence is so limited as to be not relevant
Second hand dealers	Not agreed - influence is so limited as to be not relevant
Telecommunications	Not agreed - Communication errors or emissions should be identified by either Built in Test or some other form of monitoring that should be the responsibility of the ADSE
Component Manufacturers	Not agreed - Vehicle configuration errors or emissions should be identified by either Built in Test or some other form of monitoring that should be the responsibility of the ADSE

Variation with Business Models - This is not agreed. The ADSE must have a single responsibility for ongoing safety that must accommodate a range of business models and third party behaviours, omissions and errors.

4. **Have we accurately described the regulation that already applies to relevant parties that would help ensure the in-service safety of automated vehicles?**

Yes - The discussion covers the existing situation suitable to support the RIS

5. **Do you think there are any new risks posed by second-hand ADS components, after-market modifications or the transfer of ownership of automated vehicles, which may not be adequately addressed by existing regulation designed for conventional vehicles?**

Yes - There are a significant number of issues that could arise that may not be covered by existing regulation and laws. However responsibility for in service safety cannot be split, attributed or contracted out. Only one party , the ADSE can be expected to be held accountable. The ADSE must have in place process and techniques to identify and manage all third party behaviours, omissions and errors.

6. **Do you think the parties with an influence on in-service safety are sufficiently covered by Australia's current legal frameworks?**

No - as discussed the ADSE must be clearly assigned sole responsibility and that responsibility must be clearly defined for the given ADS. This assignment of sole responsibility for specific outcomes is not well dealt with by either consumer law or WHS acts and should be defined in new regulation.

If existing high level laws and regulation where suitable there would be no reason for specific regulation in other like complex system industries such as rail, aviation and pharmaceuticals.

7. **Do you think that a general safety duty to ensure the safe operation of the ADS 'so far as reasonably practicable' is appropriate to address the safety risks?**

Yes - provided that this general safety duty is applied to a single entity, the ADSE and there is no multi party liability that will have the effect of diluting responsibility or accountability. If necessary there is no reason why the general safety duty cannot be clarified and focussed with some prescriptive rules and performance based regulation. As an example prescriptive rules may address requirements for some basic ADSE operating rules (e.g. a Manual of Standards for each ADSE) and some overarching performance based regulation (e.g time to advise operators, time to advise regulators) may be appropriate adjuncts.

8. **If a general safety duty were introduced, which parties should it apply to?**

The ADSE should be the sole responsible party to ensure that there is no dilution of responsibility or accountability. There should be an ADSE 'accountable manager' that incorporates the RIS concept of the ADSE executive officers. Again a single party and not a team is necessary to ensure a clear line of responsibility.

9. **If a general safety duty were introduced, should it apply on public and private land (such as residential driveways)?**

From a safety perspective the defined operating environment is the defined operating environment. The ADSE should be assigned responsibility to ensure that the ADS is not operated or cannot be operated outside of the approved operating environment.

10. **Should people injured by breaches of the duty have a cause of action, or should the ability to enforce a general safety duty be limited to a regulator?**

Third parties suffering loss or injury should remain free to seek damages from appropriate parties including the ADSE. The failure of the ADSE to meet the general safety duty can and should remain available as a rationale to seek damages and orders. These orders could include instructions to the ADSE to meet its ongoing obligations.

11. Do you think there should be specific driving rules for ADSs like the Australian Road Rules, or would it be sufficient to simply require them to 'drive safely'?

As noted because the ADS operational task is different from the human driving task it may be necessary to have the facility to make rules specific to ADS. These rules should be National not state based. The National rules could include as a minimum the requirement for the ADS to comply with all State driving rules.

12. What approach to regulating the dynamic driving task for ADSs most efficiently achieves safe outcomes? Please provide reasons.

The RIS confuses compliance with existing dynamic road rules (or developed ADS road rules) with the much more complex task of assuring in service system safety for a complex system.

Compliance with road rules, whether State or National is a minor, almost trivial, subset of the safety related behaviours of a complex ADS.

The ADS should be introduced with the support of a comprehensive safety case. Identifying deviations from that safety case is the role of the in service system safety program. The consequence of any deviations from the safety case baseline should be outlined in the safety case. The consequence of deviations should inform the response to those deviations.

The ability of the ADS to conform to existing or new dynamic driving road rules is just minor attribute of the overall ADS safety case and should be accommodated as a subset of the overarching in service safety process.

13. What functions and powers does the regulator need to effectively manage in-service safety? Would these differ depending on whether the regulator is enforcing a general safety duty, or only prescriptive duties?

14. Have we accurately described the scope of the regulatory task? Please provide data and evidence where possible to support your answer.

The ADSE is the entity responsible for ensuring the ongoing safety of the ADS. The regulator should at the highest level authorise (licence) the ADSE to perform the task and be able to remove that licence if the ADSE fails to meet its ongoing responsibilities. The role of the regulator is not impacted by either general or prescriptive duties and the following general concepts should apply.

- The regulator shall authorise the ADSE to undertake a specific scope of work with regard to a given ADS
- The regulator's authorisation shall be dependant on the ADSE developing and working to a defined set of work practices defined in a documented form (Manual of Standards - MOS)
- The MOS shall include a requirement for the ADSE to inform the regulator of deviations from the safety case accepted / approved at initial entry to service and the recommended actions to address those deviations.
- The ADSE shall be required to establish a Quality Management System (QMS) and Safety Management System (SMS) as elements of its overall operation.
- The regulator shall audit the ADSE operation and specifically look for evidence that the MOS process, the QMS audit findings and SMS audit findings are being implemented.
- The regulator shall have the authority to request ADSE corrective actions and limit the operation , if necessary, of the ADS until those corrective actions are implemented.

Based on the above model the regulatory task would be limited to review , approval and ongoing oversight of a given ADSE manual of standards, the complexity of which would vary with the complexity of the ADS and the complexity of the safety case delivered at the initial entry to service.

The number of vehicles in service or the commercial operational arrangement have limited impact on the role and responsibilities of the ADSE or the associated regulatory oversight. It is the complexity of the ADS function and the associated safety case that impacts both the ADSE operational complexity and the detailed scope and quantum of the regulatory task.

It is thought that the complexity associated with level 4 functionality is similar to level 5 functionality and hence complex safety cases and a complex ADSE function and regulatory role will exist from 2020. It is thought that from a safety assurance perspective level 3 systems are actually more complex to manage then level 4 or 5 systems due to the need to design for , monitor and manage what could be complex stochastic human behaviours and responses.

15. Have we accurately captured the benefits of the regulator being:

- **a government body or an independent body?**
- **a national body or state and territory bodies?**
- **an existing body or a new body?**

The discussion that proceeds question 15 is though to be valid with one exception.

The discussion assumes that the existing the Department of Infrastructure, Transport, Cities and Regional Development would be the entity conducting initial approval at product entry but may not have the skills to conduct in service safety assessment.

There is no objective evidence that the existing Department's responsibilities under the Road Vehicle Standards act have equipped it too in any way be involved in the assessment of new ADS into the market.

Review of the Departments existing staffing, skills base and processes to support its obligations under the act, together with its previous written and verbal input into the whole NTC process around the ADS issues suggest that it is present wholly unsuited to be involved in any aspect of initial entry review for ADS in Australia.

Given the existing significant limitations within the department is is highly likely that new staff, a new skill base, organisational culture and a new process will need to be stood up, either within the existing department or in a new regulator to support entry to service processes , regardless of the detail of the regulatory model adopted.

Accepting this premise then it is likely that the skills necessary in a new "initial entry to service" regulator will be sufficient and similar to the skills necessary to support regulation of ADSE and vice versa.

16. What are your initial views on how the regulator should be funded?

The overarching assumption of the entire ADS rollout is that these technologies will have a significant, although difficult to define, positive impact on road safety.

In the nascent stages of the rollout there is a significant risk to the social licence associated with ADS technologies , with the bulk of the risk coming from the impact of high accident rates due to the release of poor technology. Poor technology has the potential to be released due to such issues as the technical immaturity of the technologies, the organisational and cultural immaturity of the road transport industry and policing systems and the over enthusiastic expectation of investors who see ADS as some new from of industry 'disruptor' technology.

If the ADS social license is compromised in the early years then the potential community safety benefits will be delayed.

With this in mind, and given the step learning required of both industry and regulator, it is recommended that the regulator by fully publicly funded for the first decade. This will allow a regulatory method to be established and industry to understand how it works without being burdened by additional costs. The industry does not want to bear the cost of the regulator learning how to best serve the industry.

After 10 years it is proposed to transfer to a partial user pays approach to funding the regulator. It is thought that at 10 years the assumed cost reductions will have started to emerge and the overall cost benefit understanding will assist in the transfer of any costs to industry and users.

17. **Have we adequately and accurately captured the key legislative implementation models for in-service safety of automated vehicles?**

Yes the discussion in the RIS is suitable at this stage

18. **Do you think there are any transitional or constitutional issues that could arise when Australia establishes a national law for automated vehicles? If so, please explain what the issues are, and if they differ depending on the legislative implementation model used.**

Not suitably qualified to comment on this issue

19. **Have we accurately described how each option could work as well as the advantages and disadvantages of each option?**

Yes, This discussion is suitable

20. **Which option most effectively addresses the problem statement? Please consider your answer in conjunction with the PwC cost–benefit analysis.**

Option 3 best addresses the problem statement and is the preferred approach as it would seem to be the most cost effective way to implement what will be a complex new system of regulation based on the preferred general duties approaches.

The PwC cost benefit analysis has been reviewed and is not considered a sound basis for decision making as it has failed to correctly understand the nature and associated costs (for both the regulator and industry) of the necessary in service system safety regulatory process.

21. **Is there another option or combination of options which could more effectively address the problem statement? In particular, please consider whether there is a preferable combination of the elements of each option (governance arrangements, duties, legislative implementation)**

The preferred approach is general safety duties at the high level supported as necessary by some prescribed standards , which will predominantly involve process not detail safety issues. The regulation will be technically complex and require the establishment of a team of domain experts and as such is most economically executed at the national level. With these keys issues in mind Option 3 seems the appropriate option.