

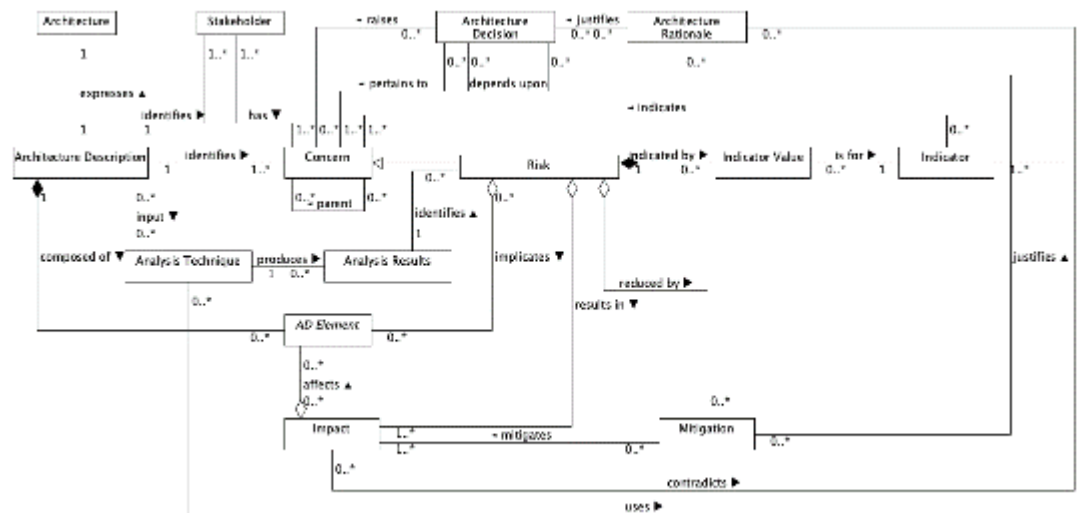
## Architecture Risk Model Research Questionnaire

### Section 1 – Participant Experience & Background

1. How many years of experience do you have in commercial software intensive systems engineering? 30
2. How many years of experience do you have in commercial software development? 8
3. How many years of enterprise architecture experience do you have? 0
4. How many years of solution architecture experience do you have? 5
5. How many years of technical architecture experience do you have? 5
6. How many years of SysML experience do you have? 0
7. How many years of UML experience do you have? 0
8. How many projects have you worked on that have involved a SysML or UML model?  
1
9. How many years do you have working with waterfall development? 30
10. How many years do you have working with agile (e.g. Scrum & SAFe) development?  
0

## Part 2 – Approach Background

The research is evaluating whether risks could be described using the following model that extends ISO 42010 – Architecture Descriptions:



ISO 42010 Concept	ISO 42010 Definition
AD element	"any construct in an architecture description." (p. 7)
Architecture	"fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution." (p.8)
Architecture Decision	"pertain to system concerns; however, there is often no simple mapping between the two. A decision can affect the architecture in several ways." (p. 7)
Architecture Description	"work product used to express an architecture." (p. 2)
Architecture Model	"uses modelling conventions appropriate to the concerns to be addressed." (p. 6)
Architecture Rationale	"records explanation, justification or reasoning about architecture decisions that have been made." (p. 7)
Architecture View	"work product expressing the architecture of a system from the perspective of specific system concerns." (p. 2)
Architecture Viewpoint	"work product establishing the conventions for the construction, interpretation and use of architecture views to frame specific system concerns." (p. 2)
Concern	"interest in a system relevant to one or more of its stakeholders." (p. 2)
Correspondence	"defines a relation between AD elements." (p. 7)
Correspondence Rule	"enforce relations within an architecture description (or between architecture descriptions)." (p. 7)
Model Kind	"conventions for a type of modelling." (p. 2)
Stakeholder	"individual, team, organization, or classes thereof, having an interest in a system." (p. 2)
System-of-interest	"systems that are man-made and may be configured with one or more of the following: hardware, software, data, humans, processes (e.g., processes for providing service to users), procedures (e.g. operator instructions), facilities, materials and naturally occurring entities." (p. 3)
Extension Concept	Extension Definition
Risk	Sub type of <b>Concern</b> that represents a <b>Risk</b> , e.g. error-proneness or security vulnerability.
Indicator	Indicates the relative risk of a <b>Risk</b> . An <b>Indicator</b> could be a quantitative software engineering metric such as a coupling measure or a qualitative assessment by an architect.
Indicator Value	The value of a particular <b>Indicator</b> for a particular <b>Risk</b> .
Impact	Represents a potential consequence of a <b>Risk</b> being left untreated.
Mitigation	Represents an action that could be taken to reduce the potential <b>Impact</b> of a <b>Risk</b> .
Analysis Technique	Identifies the architecture analysis technique used to for a risk analysis.
Analysis Results	Encapsulates the results of a risk analysis performed using an analysis technique.

## Part 3 – Approach Examples

### **Example 1 - Excessive Change Propagation**

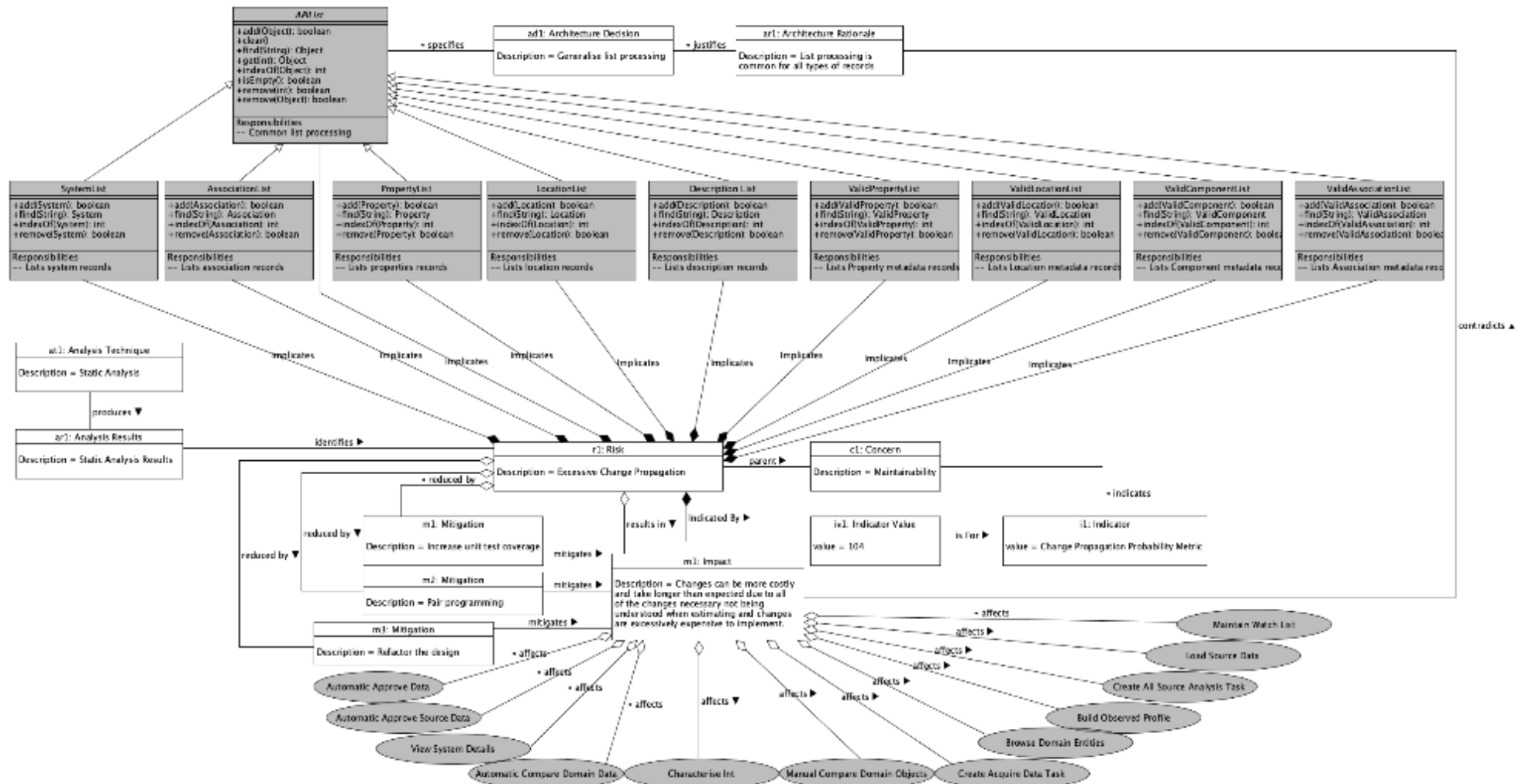
#### **Text Risk Description**

Title:	Excessive change propagation
Details:	Complex concrete sub-classes have emerged from the diverse use cases the lists had to support. E.g. SystemList needs “deleted record processing” whereas PropertyList does not. This causes conflicts between abstract class code and concrete sub-class code. This could be considered an unhealthy inheritance tree. There are also some common complex routines that are not always abstracted so when bugs have to be fixed sometimes many List sub-classes had to be changed.
Impact:	Changes can be more costly and take longer than expected due to all of the changes necessary not being understood when estimating and changes are excessively expensive to implement.
Mitigations:	Increase test coverage, pair programming, refactor the design

## Risk Model Representation

Notes:

- Grey background elements indicate elements from the design model;
- White background elements are elements added from the proposed risk model.



## Example 2 - 3<sup>rd</sup> Party Interface Changes outside of MASS control

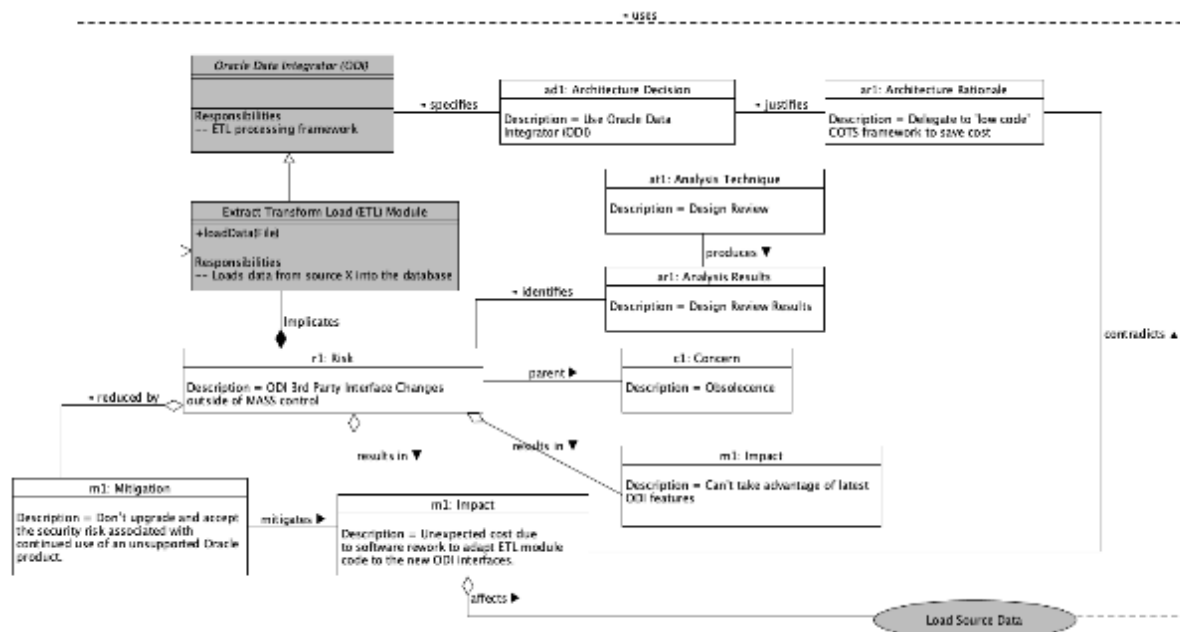
### Text Risk Description

**Title:** Low code framework Interface Changes outside of MASS control  
**Details:** Oracle Data Integrator (ODI) has changed its interface specification. This will require MASS code to be reworked if ODI has to be upgraded.  
**Impact:** Unexpected cost due to software rework to adapt ETL module code to the new ODI interfaces. Can't take advantage of latest ODI features.  
**Mitigation:** Don't upgrade and accept the security risk associated with continued use of an unsupported Oracle product.

### Risk Model Representation

Notes:

- Grey background elements indicate elements from the design model;
- White background elements are elements added from the proposed risk model.



Part 4 – Risk Model Evaluation Questions

#	Question	Answer (Delete Y / N / Not Sure as appropriate)			Comments – Please include any qualifying statements
		Waterfall	Agile e.g. Scrum	Scaled Agile e.g. SAFe	
11.	Do you think the proposed risk model would help design reviews?	Y	Y	Y	<p>The software development lifecycle model adopted will influence the Architectural Design development and identification of technical risks from analysing the AD.</p> <p>Waterfall: the AD is fully developed upfront so technical risks are identified upfront, reviewed and assessed once (typically, until a Requirements Change arrives).</p> <p>Scrum/SAFe: the initial, outline AD is developed and extended incrementally as the AD is fleshed out to address new features/functions introduced by subsequent Sprints. Likewise the number of technical risks identified will grow as the AD grows.</p> <p>IF the Design Review and its technical risk review activity also re-assesses pre-assessed AD architecture then there is a greater chance of picking up technical risks not picked up earlier, or identifying new technical risks within existing architecture as a consequence of introducing new architecture or features/ requirements with unseen dependencies/ consequences on existing AD elements.</p>
12.	Do you think the proposed risk model could help to identify risks?	Y	Y	Y	<p>The ARModel forces the Ent/Soln Architect to address technical risks as they have to define and map them out ... rather than treating them as an afterthought and adding to the Risk Register when they get around to it.</p> <p>Also, the AD model will need to be supported by a technical risk modelling entity/register to hold the outputs of the AR modelling and analysis activity. I don't recall ever seeing such an entity in an Enterprise Architect model to date.</p>

13.	Do you think the proposed risk model could help the analysis of identified risks?	Y	Y	Y	<p>The ARModel forces Ent/Soln Architect and reviewers to think about technical risk as the Ent/Soln Architect has to define and map them out as part of the AD activity.</p> <p>Is notation correct? “m1: Mitigation” and “m1: Impact” – should it be “i1: Impact”?</p>
14.	Do you think the proposed risk model could help with the assessment of analysed risks?	Y	Y	Y	<p>You can’t assess risks if you don’t identify them in the first place. Given the ARModel looks at Concerns, Mitigations, Impacts of given risks producing results, then yes, I do think it will significantly improve technical risk assessment.</p> <p>NB: there’s no mention of the Probability aspect of risk assessment though...</p>
15.	Do you think the proposed risk model could help the mitigation of assessed risks?	Y	Y	Y	<p>You can’t mitigate risks if you don’t identify them or assess them correctly in the first place.</p> <p>Given the ARModel forces Ent/Soln Architect and reviewers to assess technical risks and derive Mitigations where identified, then yes, I do think it will significantly improve technical risk mitigation development.</p>
16.	Do you think the proposed risk model could help monitoring of ongoing risks?	Not Sure	Not Sure	Not Sure	<p>Risk Monitoring appears to be out of scope of the ARModel (Part 2 top diagram) – there’s no link or trigger for when the AD and ARModel outputs are actively reviewed and assessed through lifecycle stage/design reviews (PDR/CDR or Integration Readiness reviews) or Sprint Retrospectives, etc.</p>
17.	Do you think the proposed risk model could be useful when a design model doesn’t exist?	Not Sure	Not Sure	Not Sure	<p>Doesn’t look like it. If the ARModel was extended to include Requirements then it would be applicable when assessing Use Cases etc. within e.g. Enterprise Architect modelling of requirements.</p> <p>I’m assuming a ‘design model’ is referring to an AD model and not to a lower-level DD model existing to support/extend the AD</p>

					model.
#	Question				Answer – Please justify your answer with a brief explanation
18.	What do you think might be the advantages and disadvantages of modelling the risk in this way?				<p>Advantage is the ARModel forces the Ent/Soln Architect to address technical risks as they have to define and map them out ... rather than potentially treating them as an afterthought and adding to the Risk Register when they get around to it.</p> <p>Advantage is that the ARModel formally captures technical risks.</p> <p>Disadvantage is that there is an obvious cost involved as the ADModel is significantly enlarged to encompass ARModelling elements, and design reviews will take longer as each identified risk is analysed, evaluated and risk outcome agreed upon.</p>
19.	Which approach (textural description or the proposed risk model) do you prefer and why?				<p>A reviewer needs to know the syntax of the AD language when a graphical model is used. I'd suggest presenting in both formats de-risks that lack of knowledge or errors from incorrect assumptions on how to interpret the graphical model.</p>
20.	Do you think any of the entities or associations in the proposed model are unnecessary or overkill, if so which ones?				No
21.	Can you think of any entities or associations that are missing from the proposed risk model?				<p>What about Likelihood/Probability of occurrence of the risk?</p> <p>Risk evaluation of Risk Level of the risk against Tolerance Level?</p> <p>Risk Level = Probability x Impact and when Level exceeds the Tolerance Threshold it must be managed [Accept/ Tolerate   Mitigate/ Treat   Share/ Transfer   Avoid/ Terminate]</p> <p>NOTE: It appears the ARModel term 'Mitigation' could result in 1 of the 4 typical risk assessment 'Tolerate  Treat  Transfer  Terminate' options of standard risk assessment Outcomes. So there is potential confusion in use of term Mitigation within the ARModel here. Perhaps 'RA-Outcome'/ 'RT-Outcome' (Risk Assessment Outcome / Risk Treatment Outcome) is better?</p>



		<p>BS ISO 31000:</p> <p>3.7.1 risk evaluation: process of comparing the results of risk analysis (3.6.1) with risk criteria (3.3.1.3) to determine whether the risk (1.1) and/or its magnitude is acceptable or tolerable.</p> <p>3.8.1 risk treatment: process to modify risk (1.1)</p> <p>NOTE 1 Risk treatment can involve:</p> <ul style="list-style-type: none"><li>— [Terminate] avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;</li><li>— [Tolerate] taking or increasing risk in order to pursue an opportunity;</li><li>— [Terminate/Treat] removing the risk source (3.5.1.2);</li><li>— [Treat] changing the likelihood (3.6.1.1);</li><li>— [Treat] changing the consequences (3.6.1.3);</li><li>— [Transfer] sharing the risk with another party or parties [including contracts and risk financing (3.8.1.4)]; and</li><li>— [Tolerate] retaining the risk by informed decision.</li></ul>
22.	Do you have any other feedback about the proposed risk model or its usage?	<p>I think it will be highly beneficial, especially for systems/developments with high integrity, safety, security requirements or compliances.</p> <p>Looks very promising!</p>