A Thesis on Cloud Risk Governance

A classification of controls and an assessment framework for cloud risk governance maturity measurement

By: Max Boog

EY

Shape the future with confidence

The better the question. The better the answer. The better the world works.

Contents

Introduction

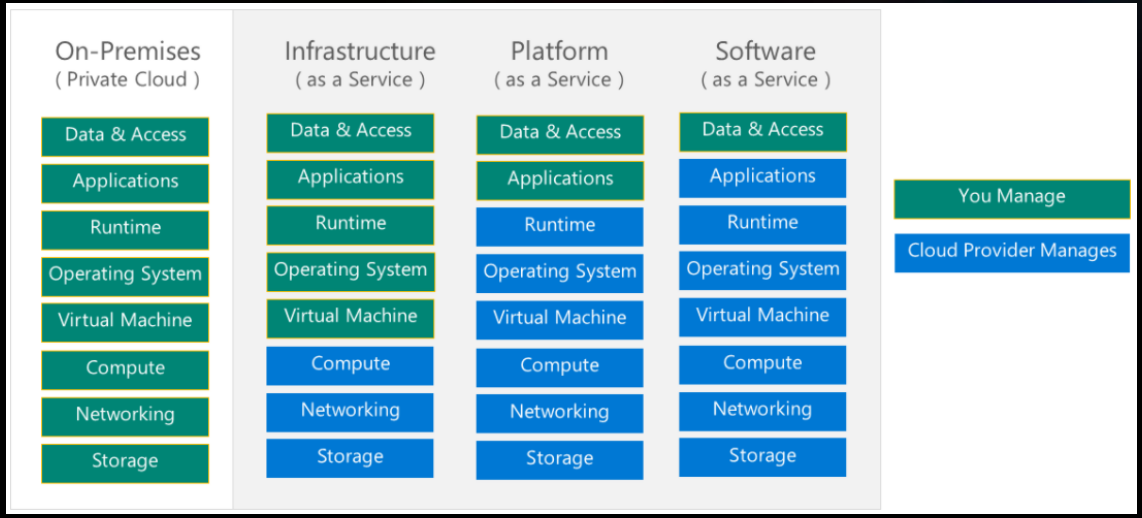
The rise of public cloud computing

- CapEx > OpEx
- Scalability and flexibility
- Faster time to market
- Making use of economies of scale
- Global infrastructure
- Easy access to advanced tech such as AI

How cloud changes the risk landscape

- Loss of direct control
- Reliance on third-parties
- Increased risks due to the elastic and dynamic nature of cloud
- Geographic and legal complexities
- **Shared responsibility**

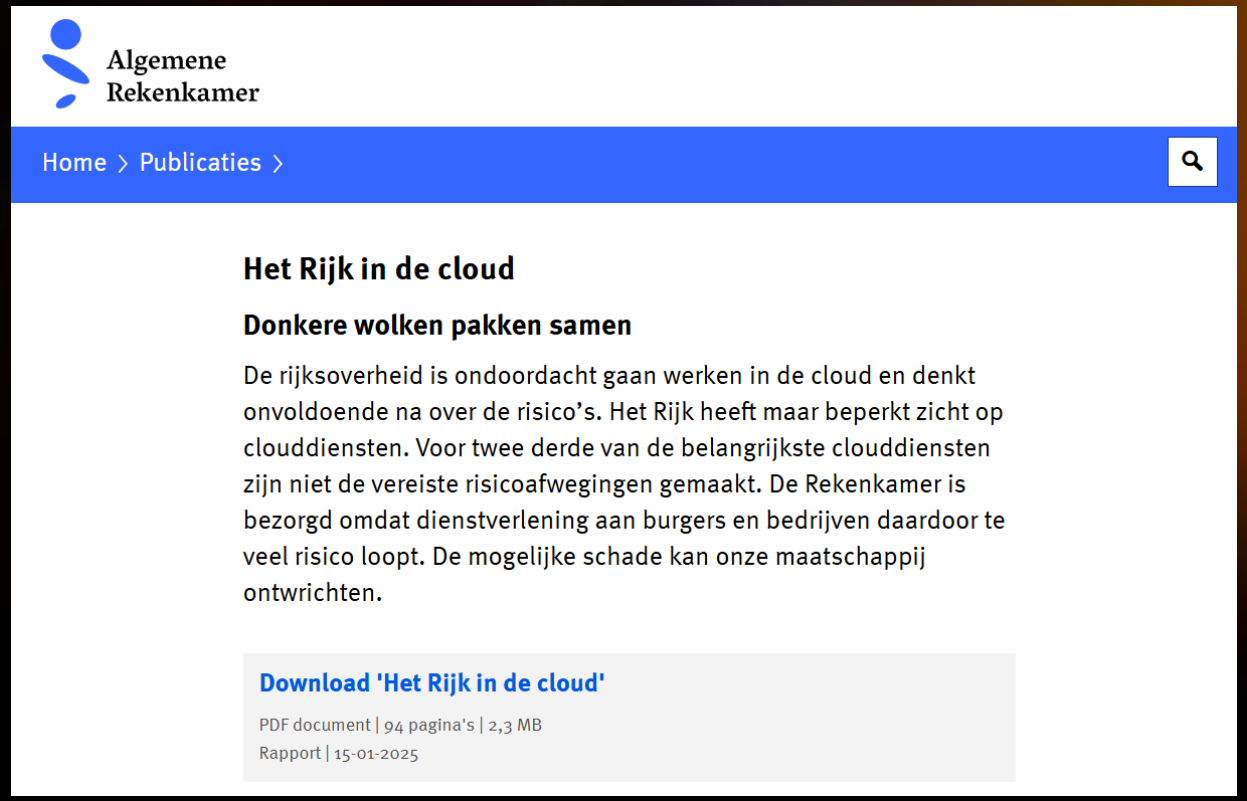
Shared Responsibility



The Challenge

- Once you are in the cloud it is hard to go back.
- Organizations do not know their responsibilities
- Organizations struggle to know where to invest limited time, resources and budget.
- No clear strategic guidance on what to prioritize in their cloud journey.
- Organizations lack practical tools to prioritize cloud risk governance improvements.

> The government has thoughtlessly started working in the cloud and is not thinking enough about the risks. The *Algemene Rekenkamer* concluded in the report *Dark Clouds Gathering* that government agencies have only limited insight into cloud services.



The Question

"How can a risk-based maturity model be developed and validated scientifically to assess an organization's cloud risk governance, incorporating expert-driven maturity classification, service model dependencies and real-world applicability?"

How can we support strategic improvement and decision making in Cloud Risk Governance?

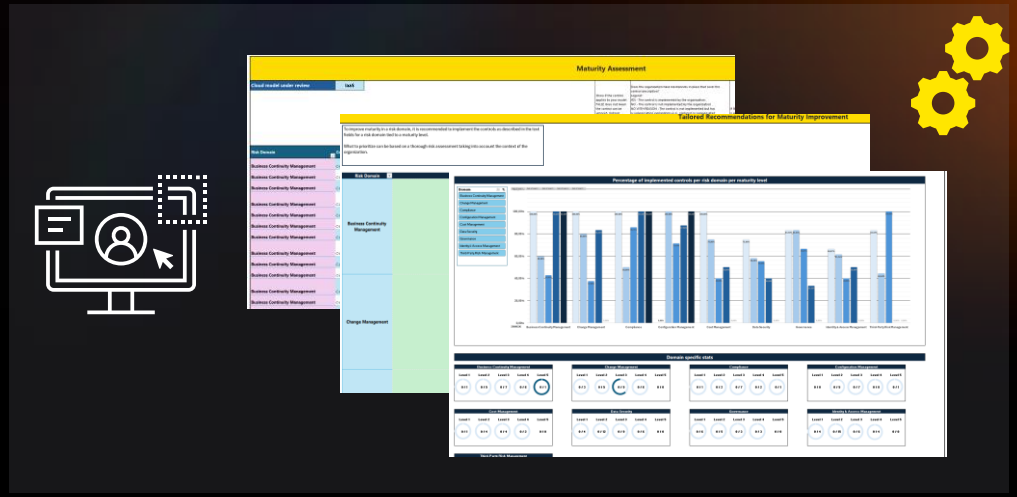
Research Objective

- Create a **progressive** maturity model for public cloud controls.

~~CMMI SM~~ ~~COBIT 2019~~ ~~NIST~~

- Scientifically validate the model based on expert consensus and a case study.

- Build a practical assessment tool that provides dashboarding and actionable insights for **strategic planning**.
- To help organizations assess their current control landscape and **identify control gaps** with what is expected at a certain maturity level.



Methodology – A three-part mixed method approach

Literature study & discovery of controls

1

Literature study

Risk domains

Control discovery

CCM Cloud Controls Matrix · NIST · CIS · ISO

Risk & Control Matrix

	CCM	ISO	CIS	NIST	IaaS	PaaS	SaaS
C-BCM-01	X				X	X	X
C-BCM-02		X	X		X	X	
C-BCM-03	X		X	X	X		
...							
C-BCM-20		X	X		X	X	

Delphi study: expert control classification in two round

2

N = 21

	Initial	Basic	Intermediate	Advanced	Specialized
C-BCM-01		> 70%			
C-BCM-02			> 70%		
C-BCM-03				>70%	

Maturity Model

Case study of the assessment tool

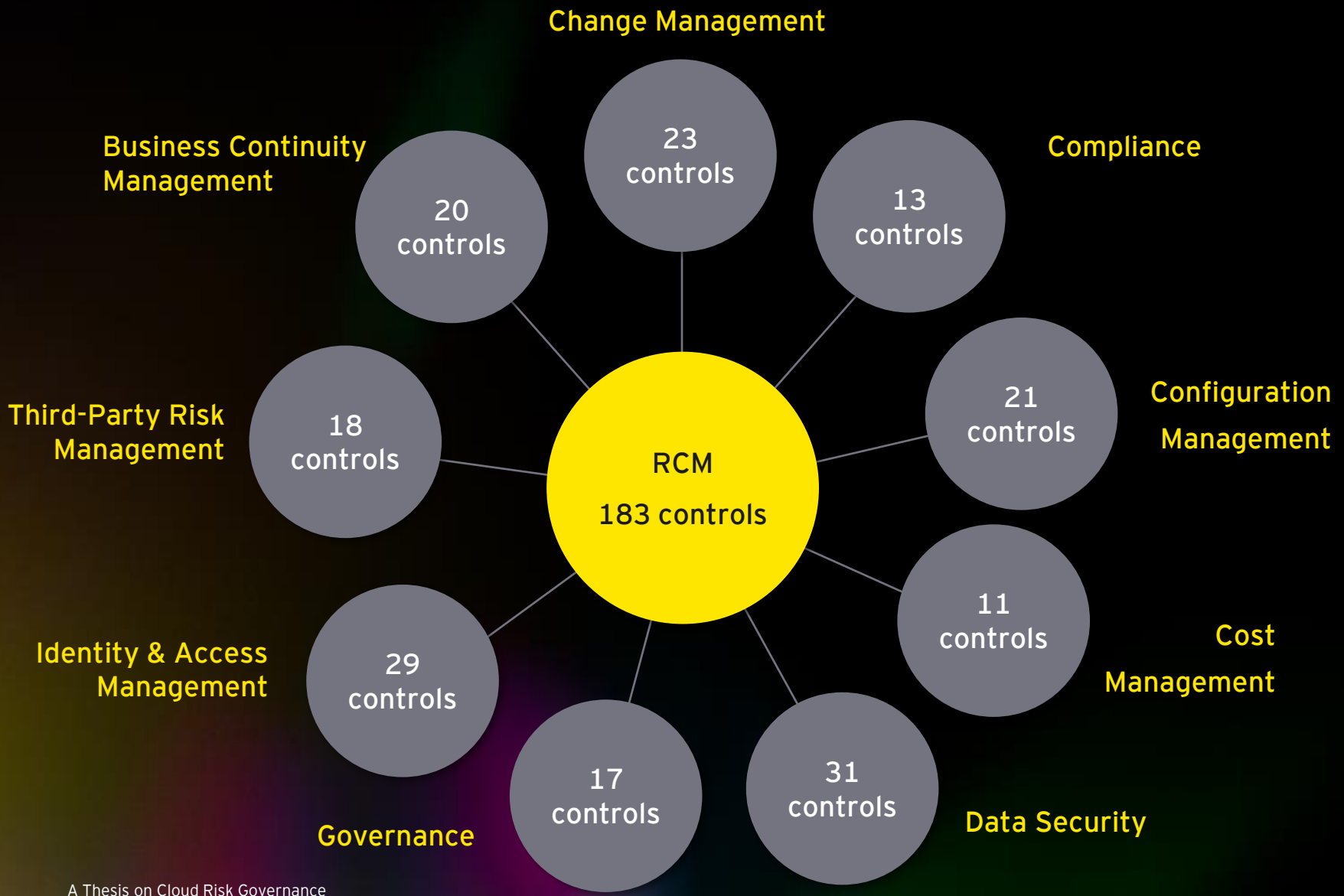
3

Assessment tool

Use case questionnaire

Adjust tool

Results – Literature study



Control classifications - Round 1

Control ID	Level 1	Level 2	Level 3	Level 4	Level 5	>70%	>60%	>50%	MODE	SD
C-BCM-01	38.1%	52.4%	9.5%	0.0%	0.0%	NO	NO	YES	2	0.52
C-BCM-02	9.5%	23.8%	52.4%	14.3%	0.0%	NO	NO	YES	3	0.82
C-BCM-03	52.4%	28.6%	19.1%	0.0%	0.0%	NO	NO	YES	1	0.45
C-BCM-04	14.3%	28.6%	57.1%	0.0%	0.0%	NO	NO	YES	3	0.75
C-BCM-05	9.5%	52.4%	33.4%	4.8%	0.0%	NO	NO	YES	2	0
C-BCM-06	4.8%	19.5%	42.9%	28.6%	4.8%	NO	NO	NO	3	0
C-BCM-07	14.3%	19.5%	42.9%	23.8%	0.0%	NO	NO	YES	3	1.29
...	...	...	...	...	...	...	...	...	...	...
C-BCM-20	0.0%	14.3%	47.6%	28.6%	9.5%	NO	NO	NO	3	0.48

Control classifications - Round 2

Control ID	Level 1	Level 2	Level 3	Level 4	Level 5	>70%	>60%	>50%	MODE	SD
C-BCM-01	23.8%	71.4%	4.8%	0.0%	0.0%	YES	YES	YES	2	0.42
C-BCM-02	4.8%	19.1%	71.4%	4.8%	0.0%	YES	YES	YES	3	0.38
C-BCM-03	57.1%	28.6%	14.3%	0.0%	0.0%	NO	NO	YES	1	0.41
C-BCM-04	9.5%	19.1%	71.4%	0.0%	0.0%	YES	YES	YES	3	0.66
C-BCM-05	9.5%	57.1%	28.6%	4.8%	0.0%	NO	NO	YES	2	0
C-BCM-06	4.8%	4.8%	85.7%	4.8%	0.0%	YES	YES	NO	3	0
C-BCM-07	9.52%	14.3%	76.2%	0.0%	0.0%	YES	YES	YES	3	0.33
...	...	...	...	...	...	...	...	...	...	...
C-BCM-20	0.0%	4.8%	90.5%	4.8%	0.0%	YES	YES	YES	3	0.32

Final consensus levels

After round 2 of the Delphi study these were the consensus percentages

The idea is that this approach is reperformable for other risk domains to extend the model.

141 out of the 183 controls

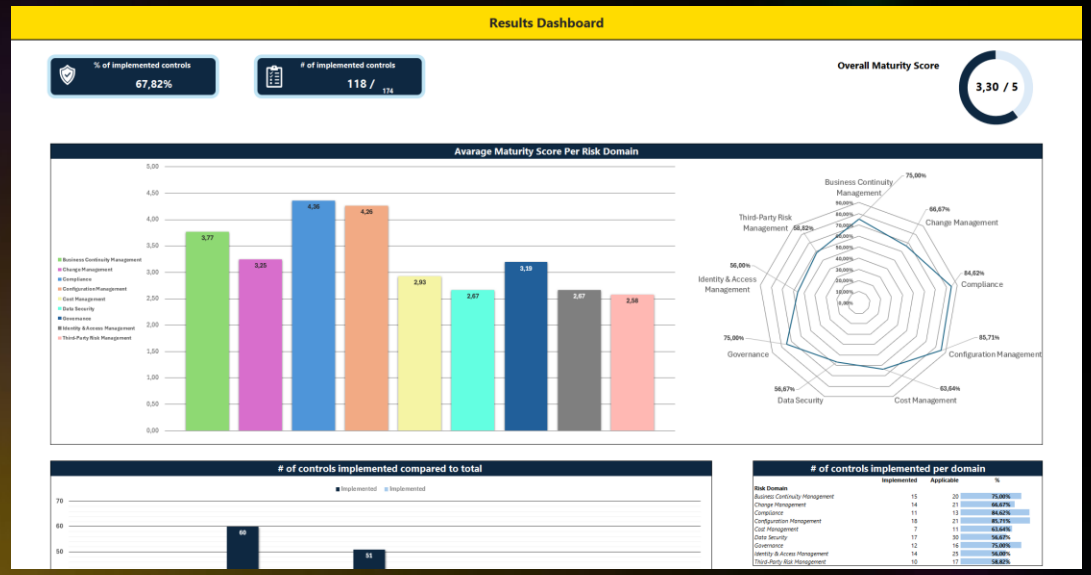
Maturity Model

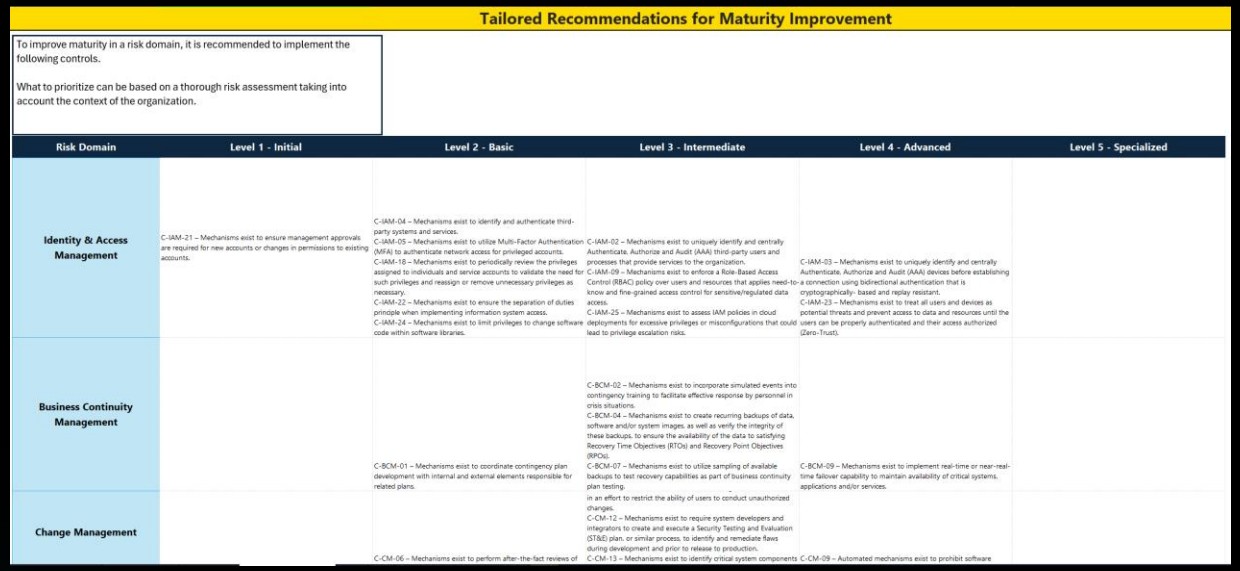
156 out of the 183 controls

183 out of the 183 controls

The assessment tool

- Insights and comparison
- What to focus on next to increase maturity in a risk domain?





What's still to come

Now

Deadline

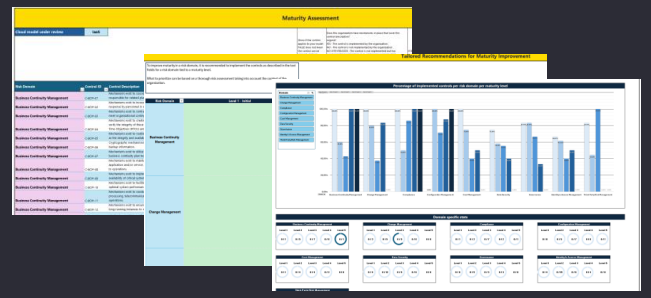
Interpretation of the results & writing

Future work

Case study

Case Study of the Assessment Tool

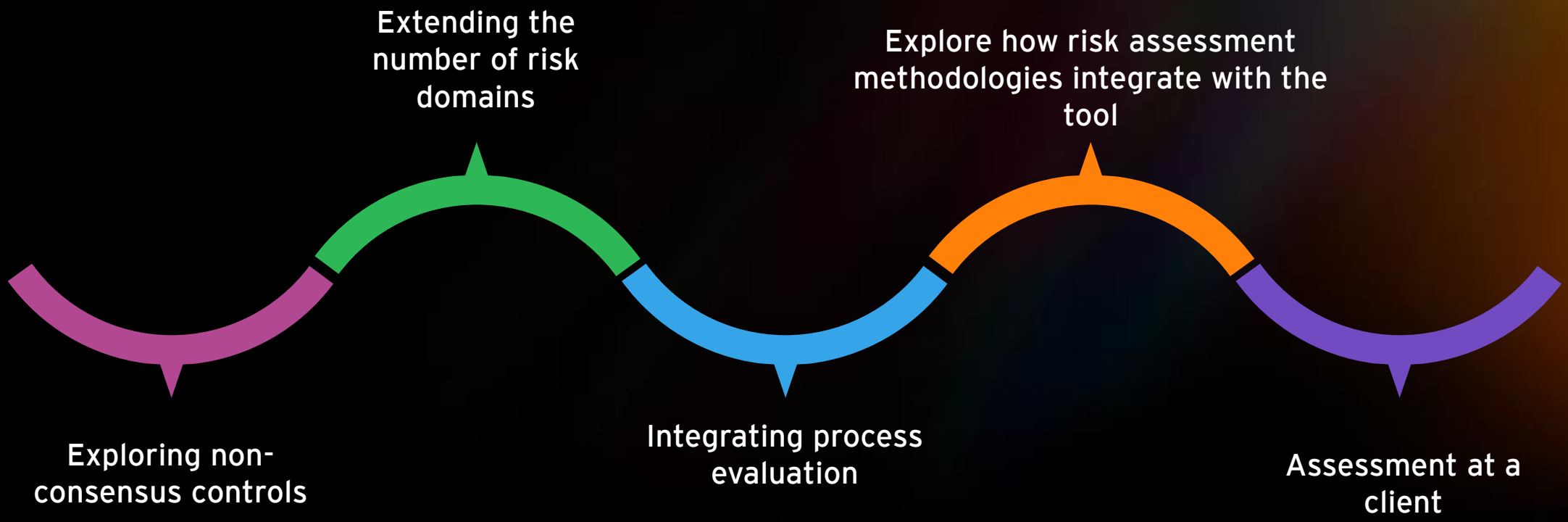
1. Maturity Assessment
2. Results
3. Tailored recommendations



Further extending the model & tool

27th of June

Outlook & Future work



Questions