

A Thesis on Cloud Risk Governance

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

By: Max Boog



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



Shape the future
with confidence

Contents

1. An Introduction to cloud computing and cloud risk

2. The Challenge

3. The Methodology

4. Results

5. What's still to come

6. Ending and questions

Introduction

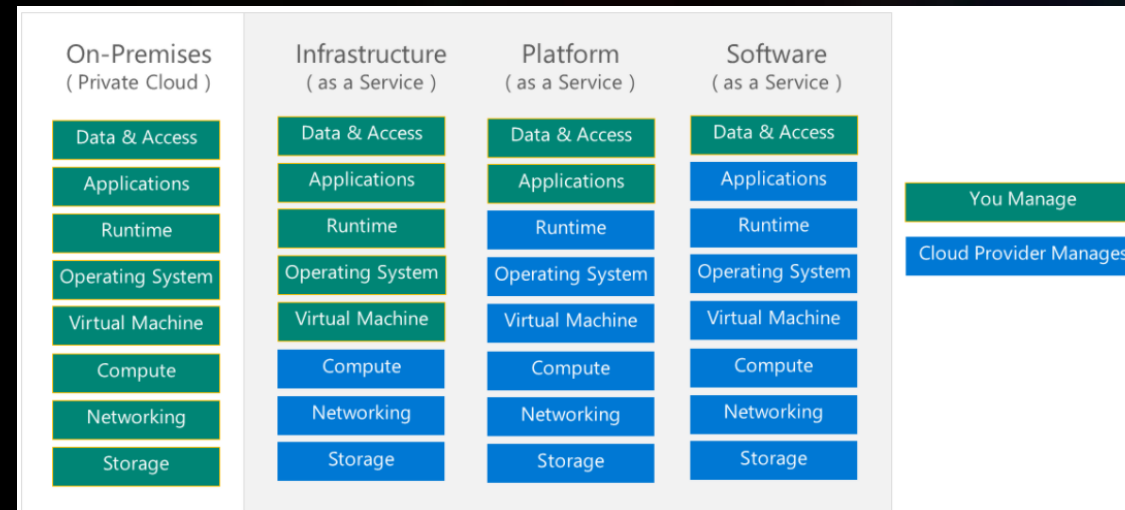
The rise of public cloud computing

- 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



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.

- 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 screenshot shows the Algemene Rekenkamer website. The header includes the logo and name 'Algemene Rekenkamer'. Below the header is a blue navigation bar with 'Home > Publicaties >' and a search icon. The main content area features the title 'Het Rijk in de cloud' and the subtitle 'Donkere wolken pakken samen'. The text describes the government's lack of oversight in cloud services and the risks involved. At the bottom, there is a button to 'Download 'Het Rijk in de cloud'' with details: 'PDF document | 94 pagina's | 2,3 MB' and 'Rapport | 15-01-2025'.

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?

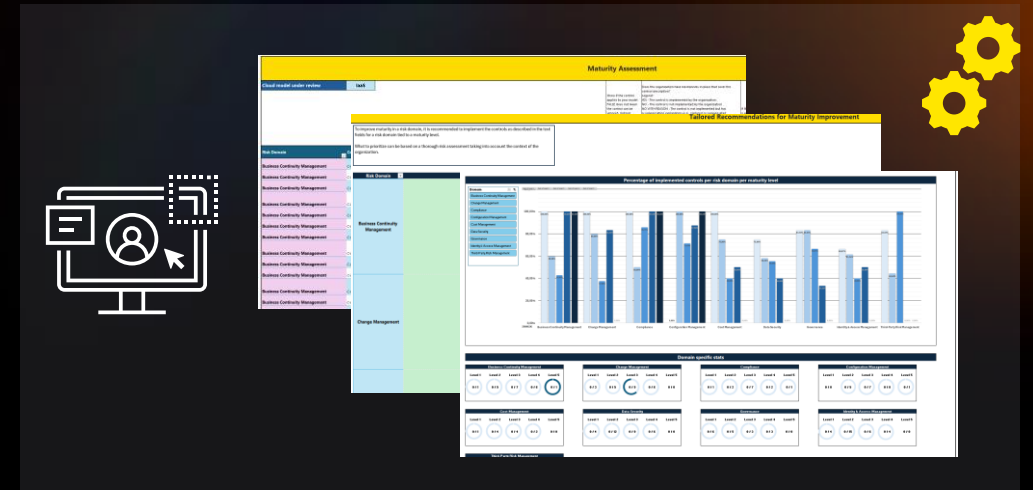
Research Objective

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



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

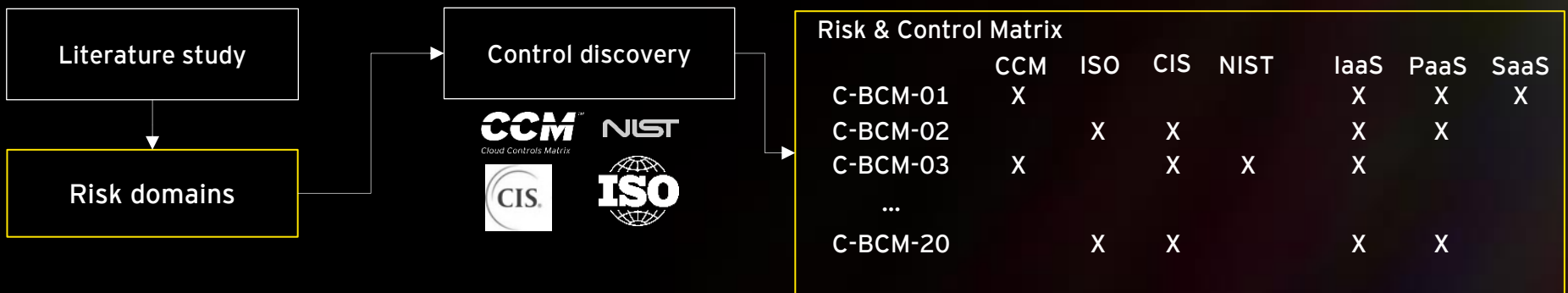
- Build a practical assessment tool that provides dashboarding and actionable insights for **strategic planning**.
- To help organizations assess their current control landscape and **identify control gaps** with what is expected at a certain maturity level.



Methodology - A three-part mixed method approach

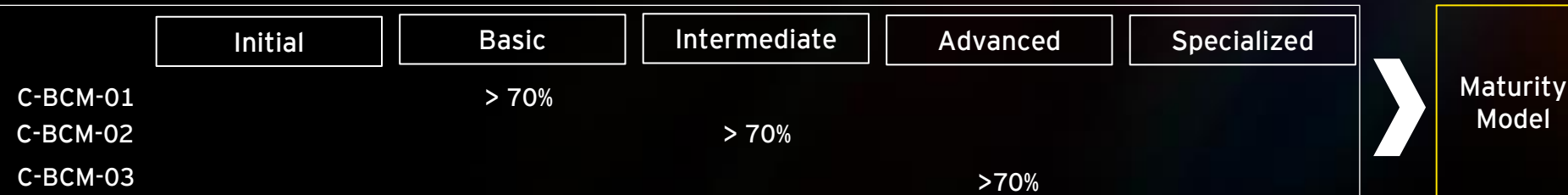
Literature study & discovery of controls

1



Delphi study: expert control classification in two round

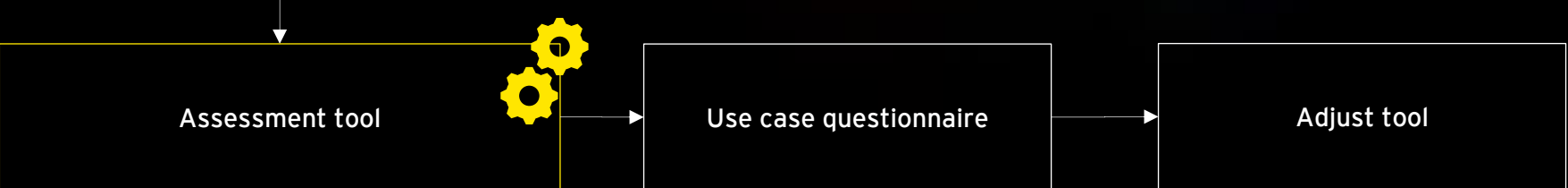
2



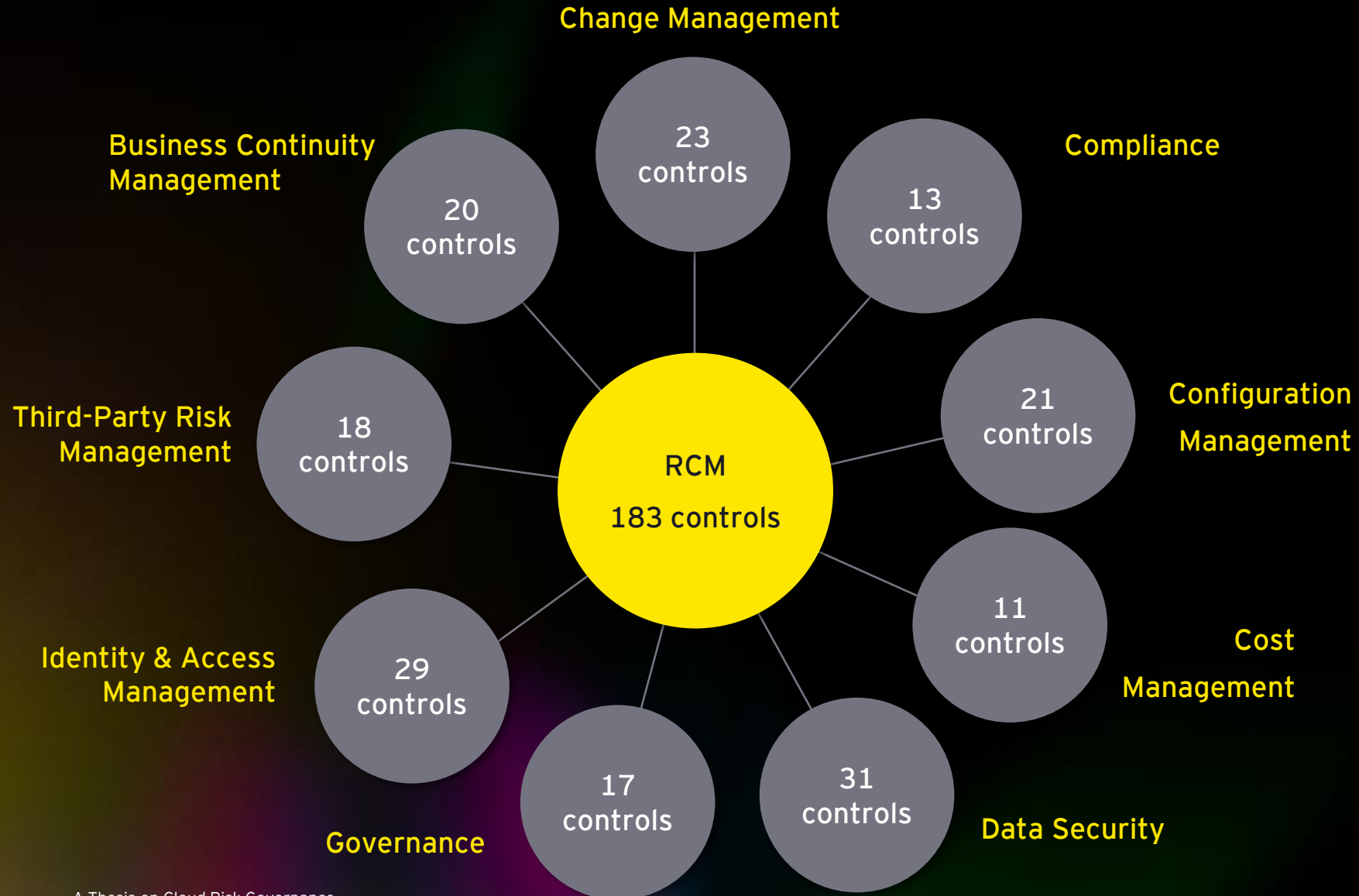
N = 21

Case study of the assessment tool

3



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

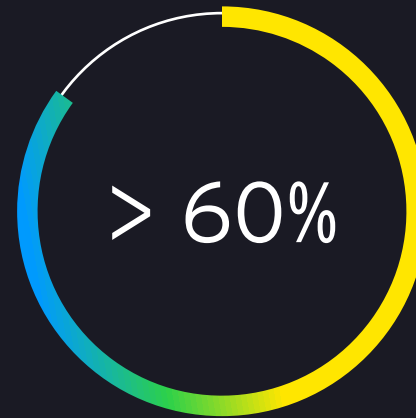
The idea is that this approach is reperformable for other risk domains to extend the model.



141 out of the 183 controls



Maturity Model



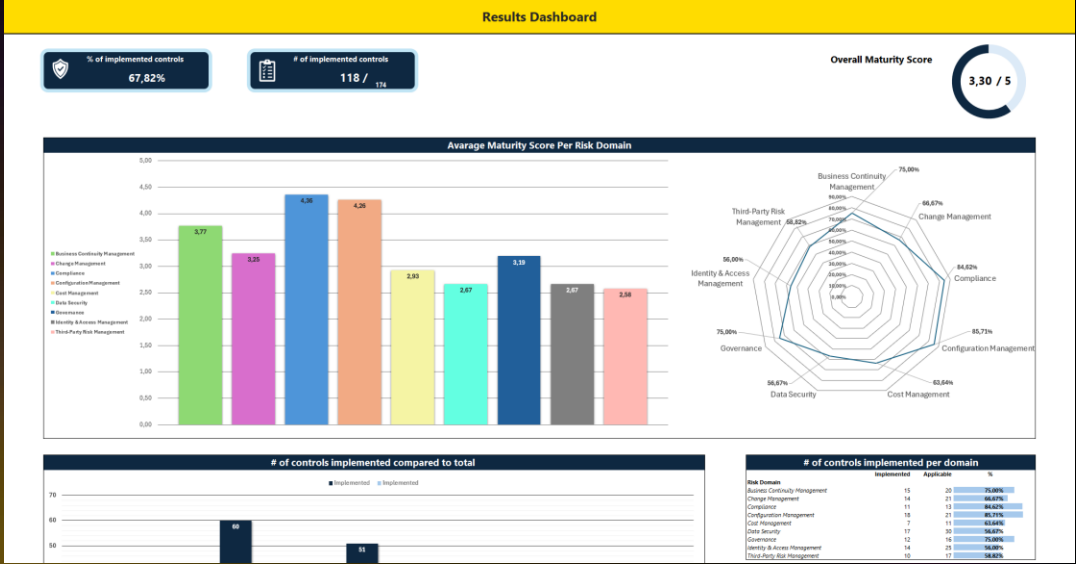
156 out of the 183 controls



183 out of the 183 controls

The assessment tool

- Insights and comparison



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

Tailored Recommendations for Maturity Improvement

To improve maturity in a risk domain, it is recommended to implement the following controls.

What to prioritize can be based on a thorough risk assessment taking into account the context of the organization.

Risk Domain	Level 1 - Initial	Level 2 - Basic	Level 3 - Intermediate	Level 4 - Advanced	Level 5 - Specialized
Identity & Access Management	C-IAM-21 – Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.	C-IAM-04 – Mechanisms exist to identify and authenticate third-party systems and services. C-IAM-05 – Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts. C-IAM-18 – Mechanisms exist to periodically review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges as necessary. C-IAM-22 – Mechanisms exist to ensure the separation of duties principle when implementing information system access. C-IAM-24 – Mechanisms exist to limit privileges to change software code within software libraries.	C-IAM-02 – Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization. C-IAM-09 – Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulatory data access. C-IAM-25 – Mechanisms exist to assess IAM policies in cloud deployments for excessive privileges or misconfigurations that could lead to privilege escalation risks.	C-IAM-03 – Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically-based and replay resistant. C-IAM-23 – Mechanisms exist to treat all users and devices as potential threats and prevent access to data and resources until the users can be properly authenticated and their access authorized (Zero-Trust).	
Business Continuity Management			C-BCM-02 – Mechanisms exist to incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations. C-BCM-04 – Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). C-BCM-07 – Mechanisms exist to utilize sampling of available backups to test recovery capabilities as part of business continuity plan testing. C-BCM-12 – Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development and prior to release to production.	C-BCM-09 – Mechanisms exist to implement real-time or near-real-time failover capability to maintain availability of critical systems, applications and/or services.	
Change Management			C-CM-06 – Mechanisms exist to perform after-the-fact review of	C-CM-13 – Mechanisms exist to identify critical system components	C-CM-09 – Automated mechanisms exist to prohibit software

What's still to come

Now



Interpretation of
the results &
writing

Deadline



Future work →

Case study



Further
extending the
model & tool

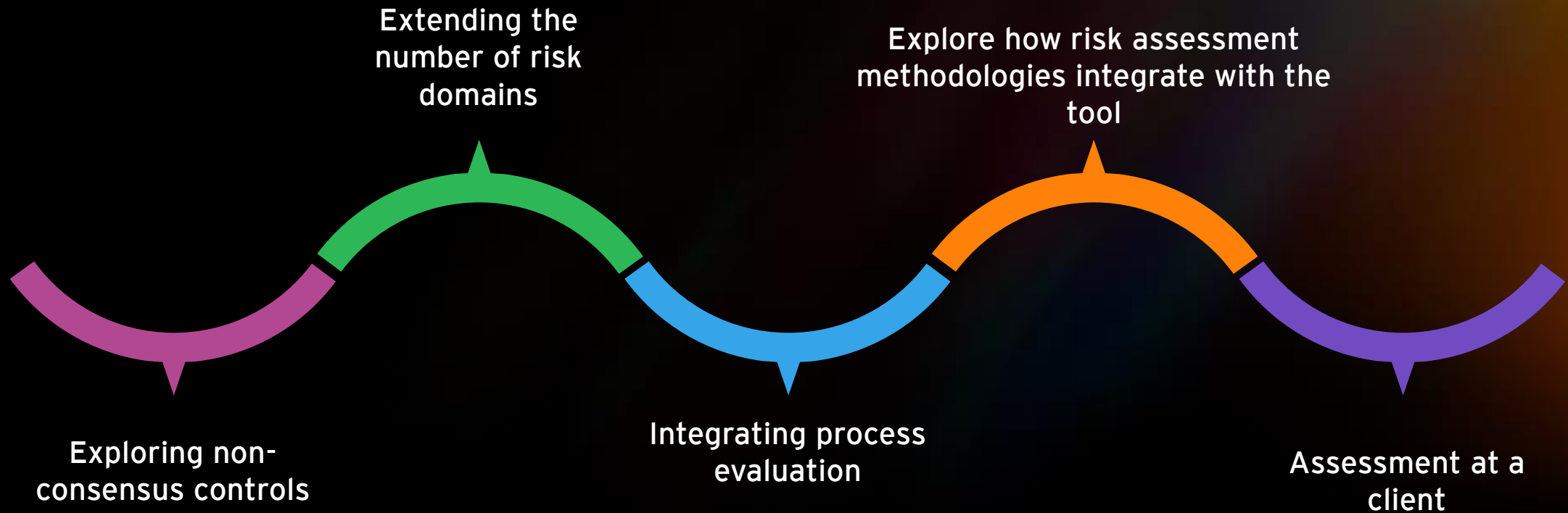
27th of June

Case Study of the Assessment Tool

- 1. Maturity Assessment
- 2. Results
- 3. Tailored recommendations

The screenshot displays the 'Maturity Assessment' tool interface. It features a table with columns for 'Business Unit', 'Maturity Level', and 'Recommendations'. The table lists various business units and their corresponding maturity levels. To the right of the table, there is a bar chart showing the distribution of maturity levels across different business units. The interface is clean and professional, with a dark background and white text.

Outlook & Future work



Questions

