

HANFA Community Orbit Security Analysis

November 2025

About us



Edward Starkie

Director, Cyber Risk

- Consultant specialising in business focused cyber security, compliance and resilience.
- Heavily focused on leveraging threat intelligence and providing pragmatic advice for business leaders on how to achieve long term objectives.
- A full member of the Chartered Institute of Information Security (CIIISec).
- A certified Information Security Manager (CISM).
- Previous experience includes Kroll, PwC, Shell, Ds Smith, Royal Mail.
- London based but with a global portfolio of clients.



Shreeji Doshi

Director, Cyber Risk

- Has more than 15 years of experience in multiple information security domains and frameworks enabling him to support clients in managing their risks by designing and implementing appropriate solutions and governance practices.
- Has experience in regulatory frameworks, with a particular focus on the Digital Operational Resilience Act (DORA) and the Network and Information Security Directive 2 (NIS2). He has supported clients in achieving compliance and has been an active speaker at industry conferences and webinars.
- Prior to joining Thomas Murray, Shreeji worked at Kroll; prior to that at EY where he worked for 11 years in India and Europe.

Full service offering

Bringing the best of our collective experience, energy and creative power to safeguard our clients and their communities.

- **Respond**
Respond to unexpected events, preserving reputation and value
- **Improve**
Understand your risk profile based on real world factors
- **Secure**
Defend against known and unknown threats
- **Quantify**
Plan continuous improvement using our knowledge of real-world events





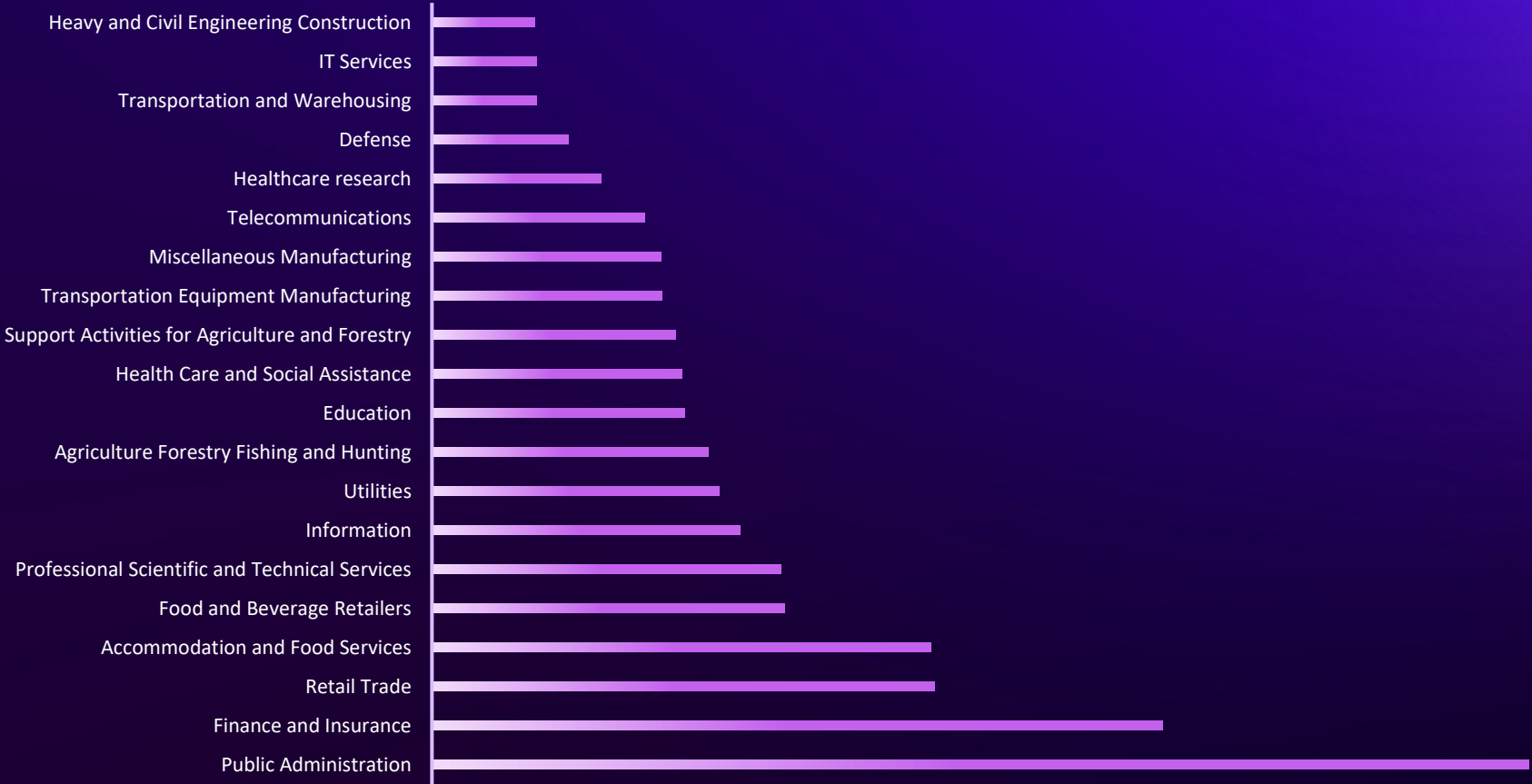
01

Context

A word cloud of terms related to cyber risk and financial services regulation. The words are arranged in a circular pattern, with some terms appearing more frequently than others. The colors of the words range from light blue to dark blue. The terms include:

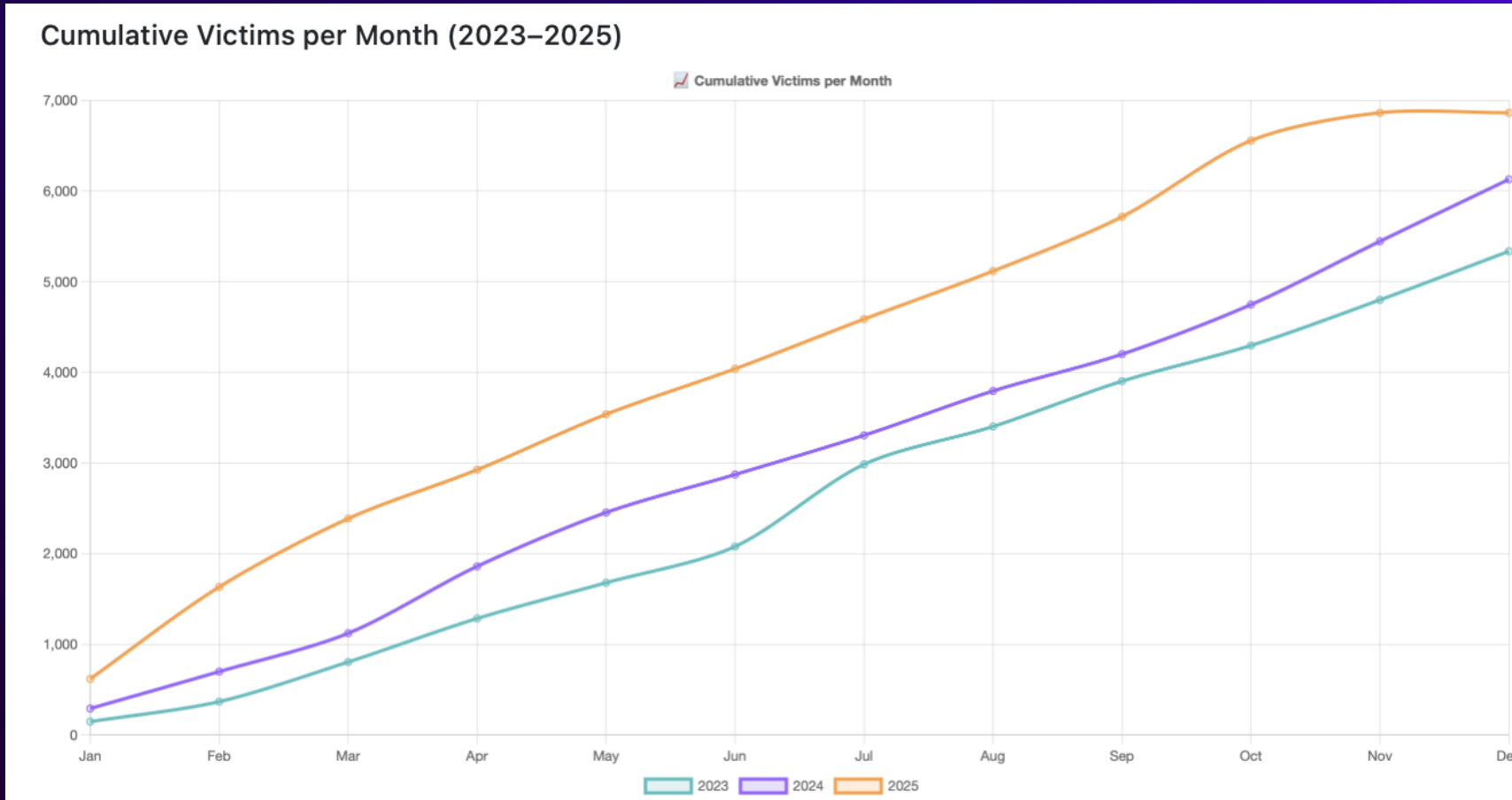
- digital oversight
- incidents
- esas
- relevant
- information
- incident
- technical
- following
- level
- business
- entity
- testing
- providers
- set
- systems
- activities
- appropriate use
- security
- referred
- regulation
- resilience
- member
- authorities
- important
- framework
- standards
- including
- point
- paragraph
- provided
- ensure
- arrangements
- entities
- shall
- ict-related
- management
- accordance
- functions
- third-party
- eu
- operational
- risk
- provider
- competent
- means
- institutions
- services
- critical data
- directive
- lead
- authority
- contractual
- overseer

Global incidents (combined TM data) 2024-2025



Source: TM data

How is ransomware doing?



Source: Ransomware Live

... It's a good business to be in

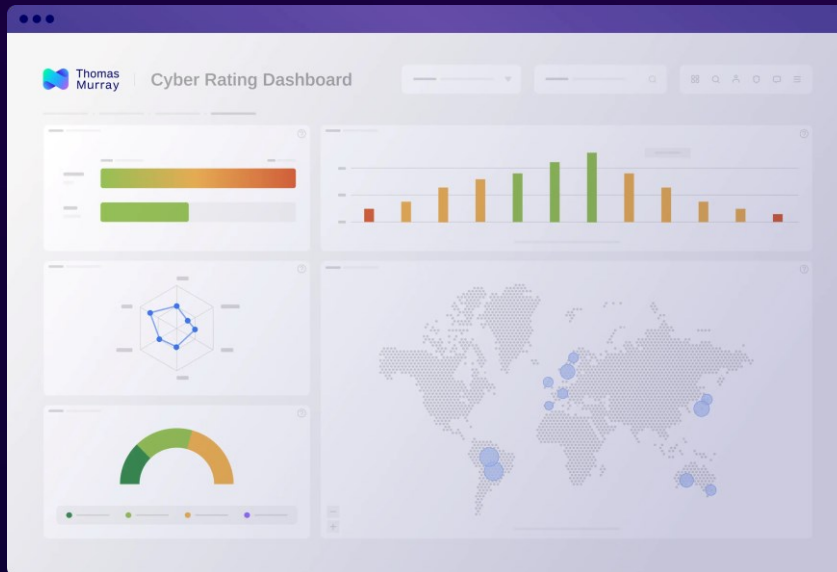


02

Orbit Security Analysis

Orbit Security

How it works



01. Provide Thomas Murray with your Root Domain(s)

02. Discover your exposed attack surface

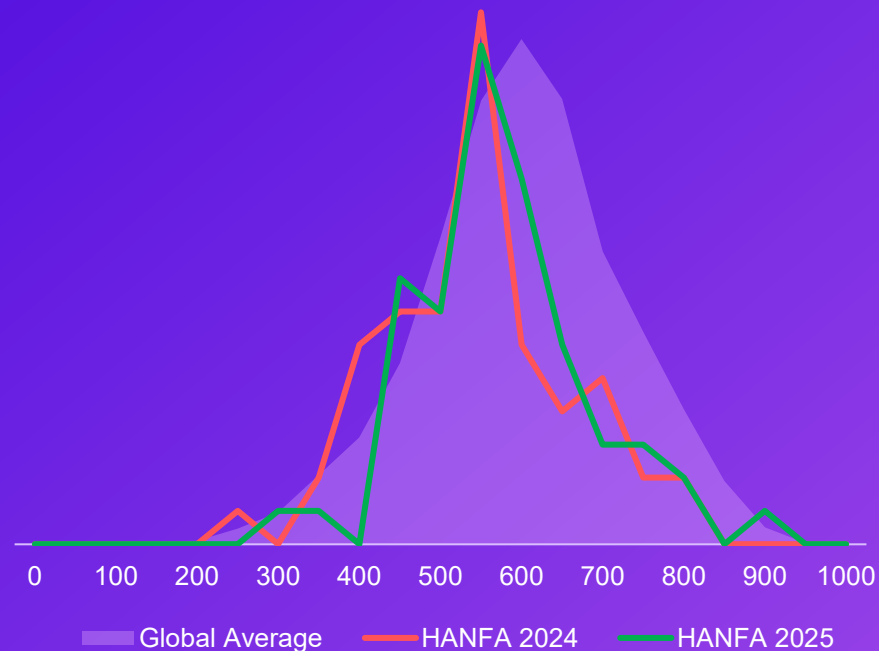
03. Continuously monitor risks, vulnerabilities, and actionable remediation information

Orbit security, vulnerability scans and penetration tests

	Orbit Security	Vulnerability Assessment	Penetration Test
Input	Domain name	IP, URL	IP, URL, application, etc
Scope	Discovering external <u>known</u> and <u>unknown</u> associated domains and sub-domains	<u>Known</u> Internal and external IP, URL	<u>Known</u> internal and external IP, URL, Application, etc.
Assessment Type	Non-intrusive	Intrusive	Intrusive and simulated attack
Explicit Permission Required	No	Yes	Yes
Assessment rating	Based on proprietary scoring methodology (0 - 1,000)	Typically based on CVSS	Typically based on CVSS with mapping to MITRE framework or custom methodology
Identification of stolen or leaked credentials	Yes	No	Yes
Identification of compromised server	Yes	No	No
Testing Cadence	Continuous	Typically, point in time activity	Typically, point in time activity

HANFA Community vs Global Benchmark

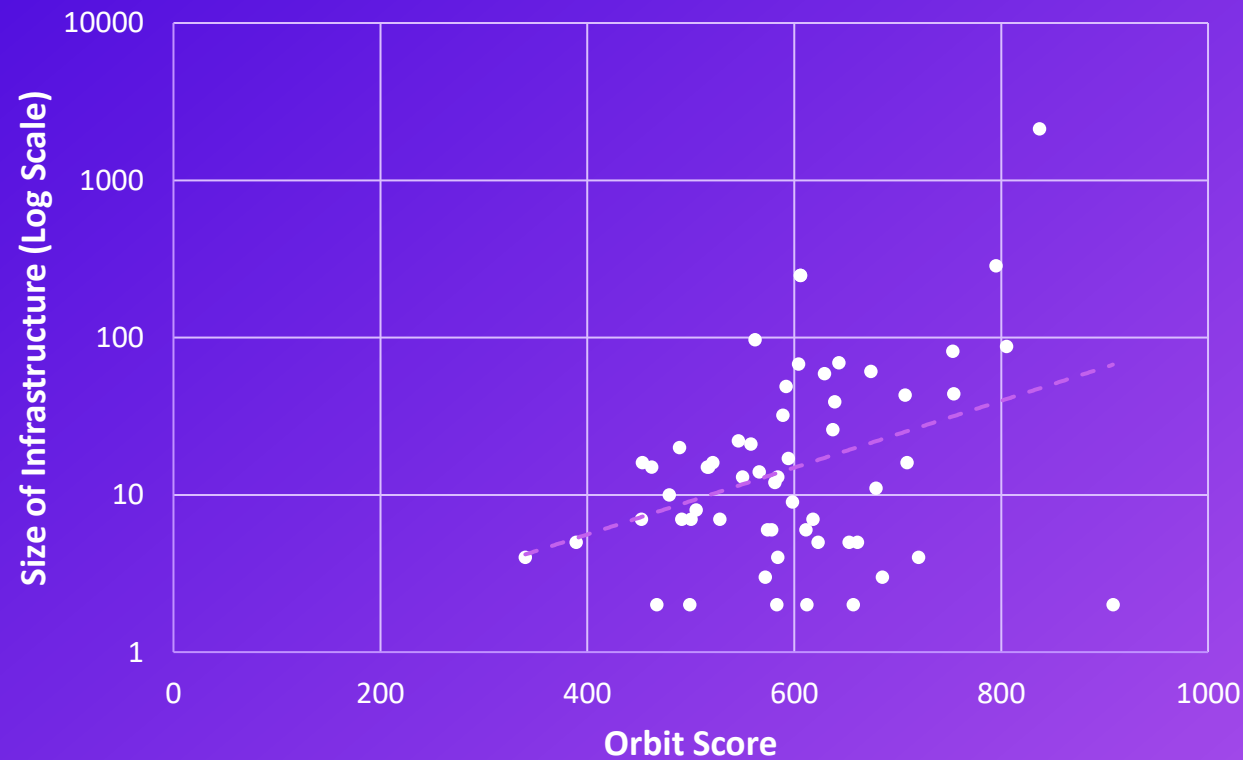
The distribution shows the number of companies at each Orbit Risk score level. The filled area represents the Global distribution of scores across all entities monitored by Thomas Murray, and the red line (2024) and green line (2025) indicates the scores in this Community



Key Takeaways:

- Overall HANFA averages have improved by around 5%
- Average HANFA community Orbit Scores:
 - 2024: 566
 - 2025 597
- This improvement brings the scores closer to the global average of 623, but still well below

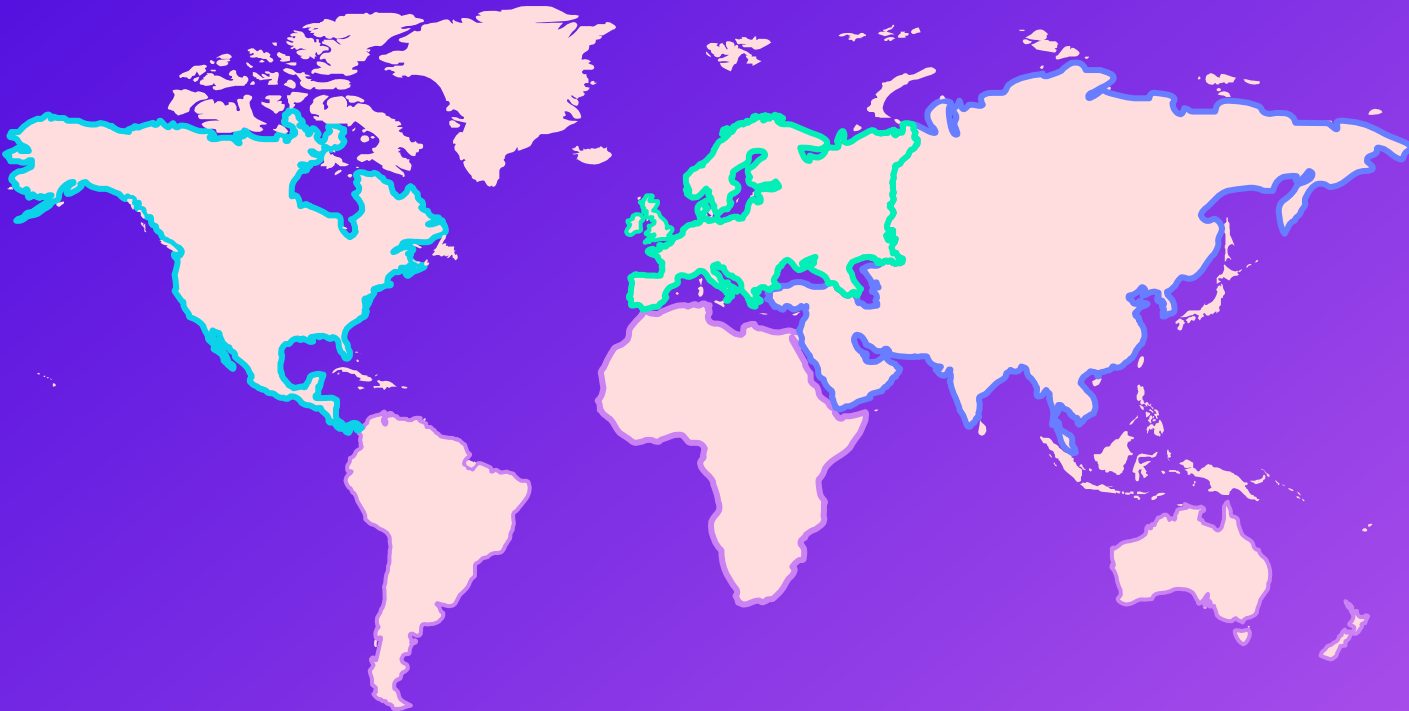
Size of Organisation vs Orbit Score



Organisations with fewer assets open to the internet generally present lower scores, as expected.

Generally, more infrastructure implies more security maturity

Geolocation of Infrastructure



81%
Europe

13%
North America

4%
Asia + ME

<1%
Other

Key Issues in HANFA Community

122

Open Service

Services likely to not be purposely exposed

27

Stolen Credentials

Stolen credentials may highlight password re-use and could be used for initial access

65

Vulnerable Service

Services out of date and may require patching

5

Compromised Server

Servers may be port-scanning or part of a botnet
– Further investigation required

Highest Risk Issues

Company A

27 cases of stolen credentials

Company B

4 potentially compromised servers

Company C

CVE-2019-13478 – CVSS Score: 9.8

Relates to: Yoast SEO plugin before 11.6-RC5 for WordPress

Company D

CVE-2017-20005 – CVSS Score: 9.8

Relates to: NGINX before

CVE-2023-44487 – EPSS Score: 93%)

Relates to: The HTTP/2 protocol

Company E

1 potentially compromised server

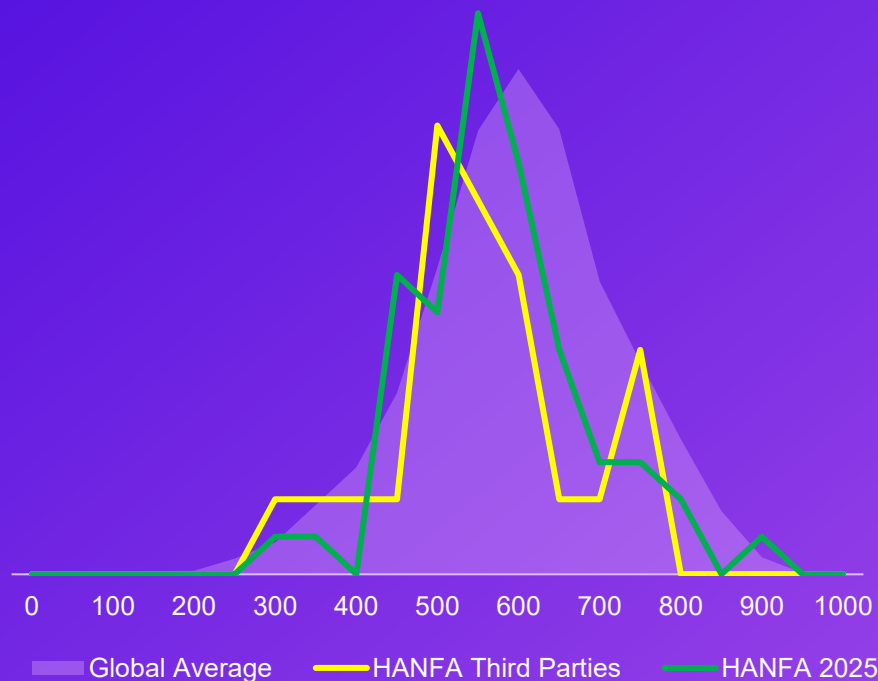


03

Third Parties

HANFA Community vs Global Benchmark

The distribution shows the number of companies at each Orbit Risk score level. The filled area represents the Global distribution of scores across all entities monitored by Thomas Murray, and the yellow line (Third Parties) and green line (HANFA Community) indicate the relevant scores

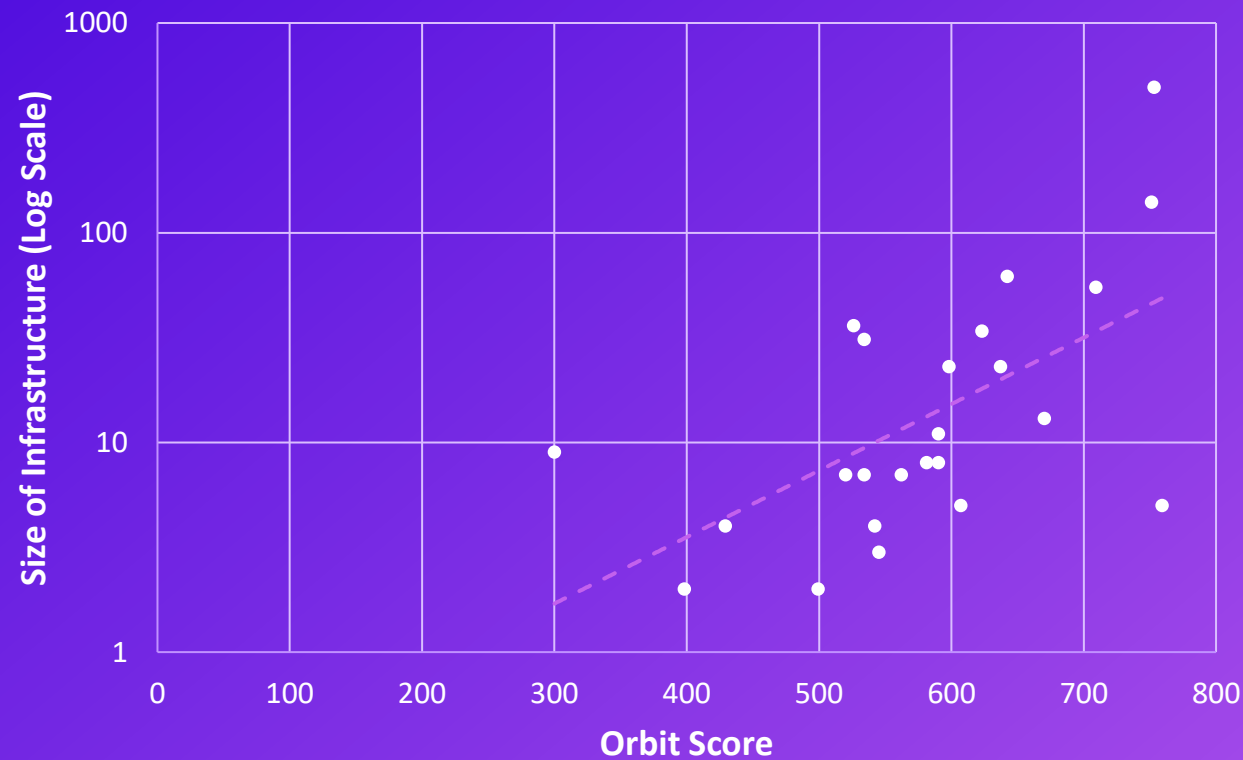


Key Takeaways:

- Overall HANFA averages have improved by around 5%
- Average community Orbit Scores:
 - HANFA: 597
 - Third Parties: 579
- HANFA Third Parties have performed below the Community at large, and also below the global average

Size of Organisation vs Orbit Score

3rd Parties



Organisations with fewer assets open to the internet generally present lower scores, as expected.

Generally, more infrastructure implies more security maturity

Key Issues in HANFA Community Third Parties

20

Open Service

Services likely to not be purposely exposed

12

Vulnerable Service

Services out of date and may require patching

What's at stake

“At £1.9 billion of financial loss, this incident appears to be the most economically damaging cyber event to hit the UK”



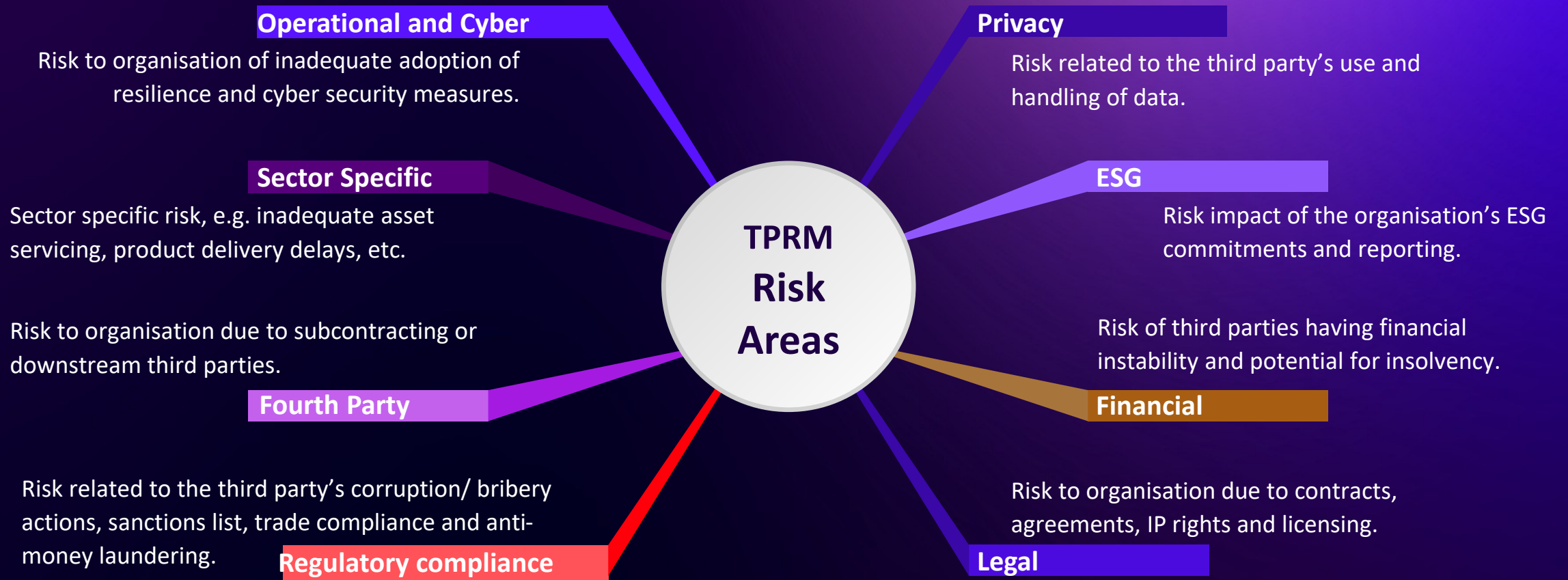
Source: <https://cybermonitoringcentre.com/2025/10/22/cyber-monitoring-centre-statement-on-the-jaguar-land-rovercyber-incident-october-2025/>



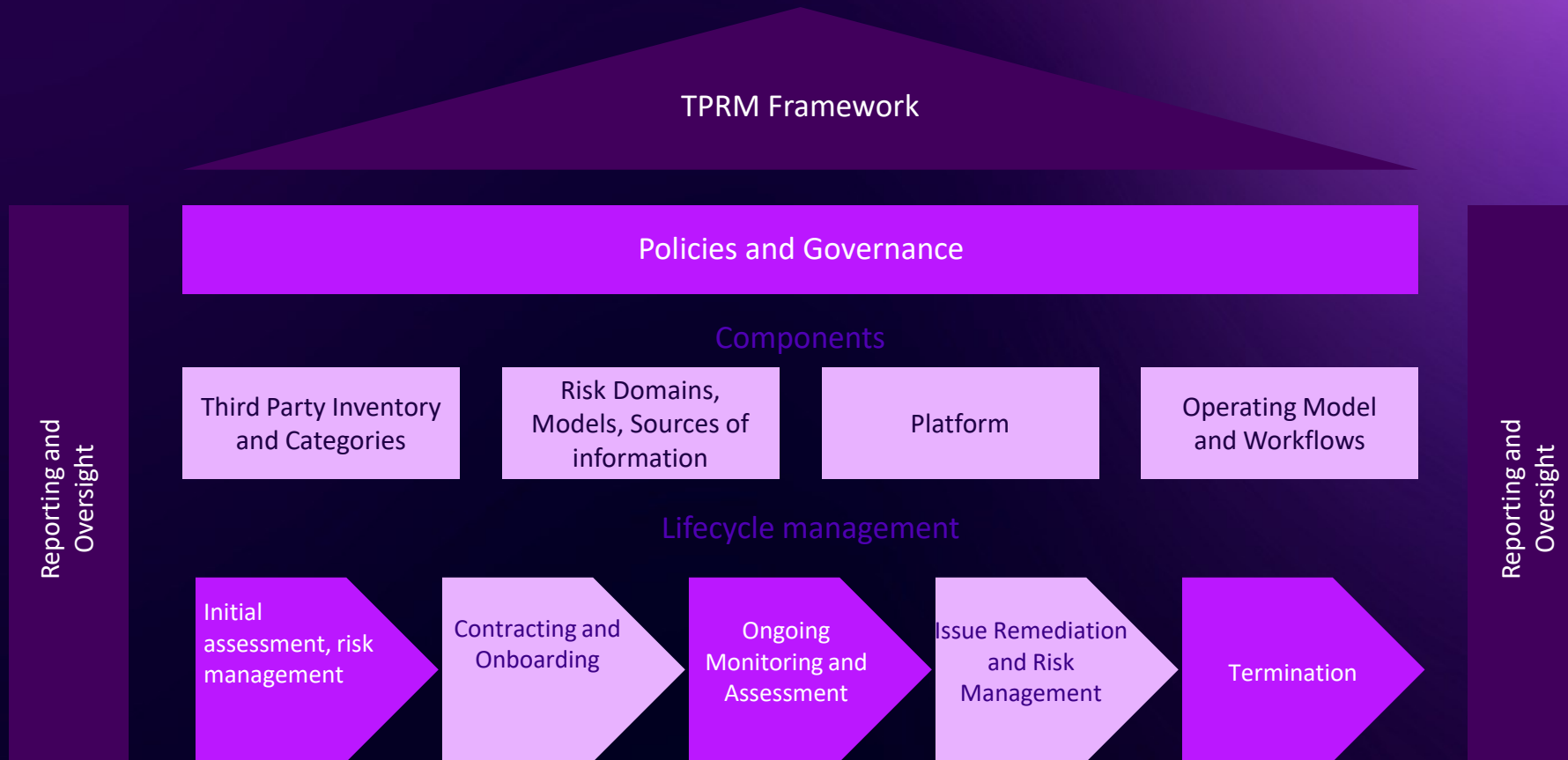
04

Managing Third party Risk

Third Party Risk Assessment Areas



Third-Party Risk Management Framework



- ✓ TPRM framework provides a structured approach to identify, assess, manage, and monitor the risks associated with third-parties.
- ✓ An effective TPRM framework requires:
 - ✓ Key aspects to ensure comprehensive risk identification, assessment, mitigation, and monitoring.
 - ✓ Governance and oversight that enables collaboration across various functions like procurement, legal, compliance, IT, and Finance across the Third-Party Lifecycle processes.
- ✓ By integrating these components into a unified framework, organizations can build a resilient TPRM program and an organisation.

Key Challenges of TPRM framework implementation

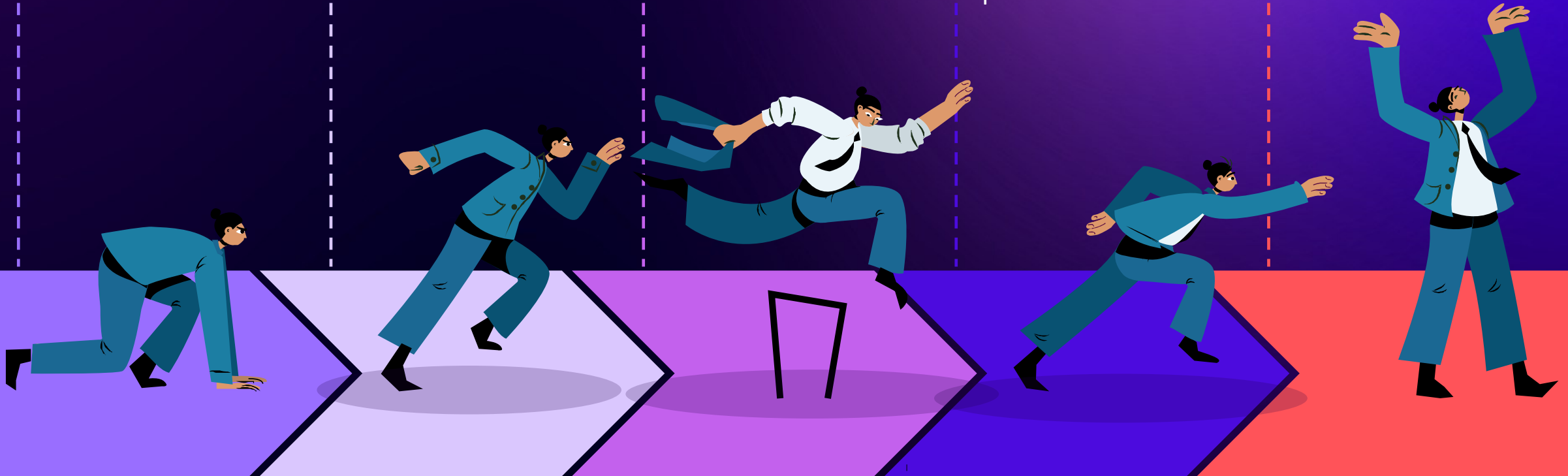
Uncertainty in identifying responsible team/ function.

Inventorying third parties and critical third parties.

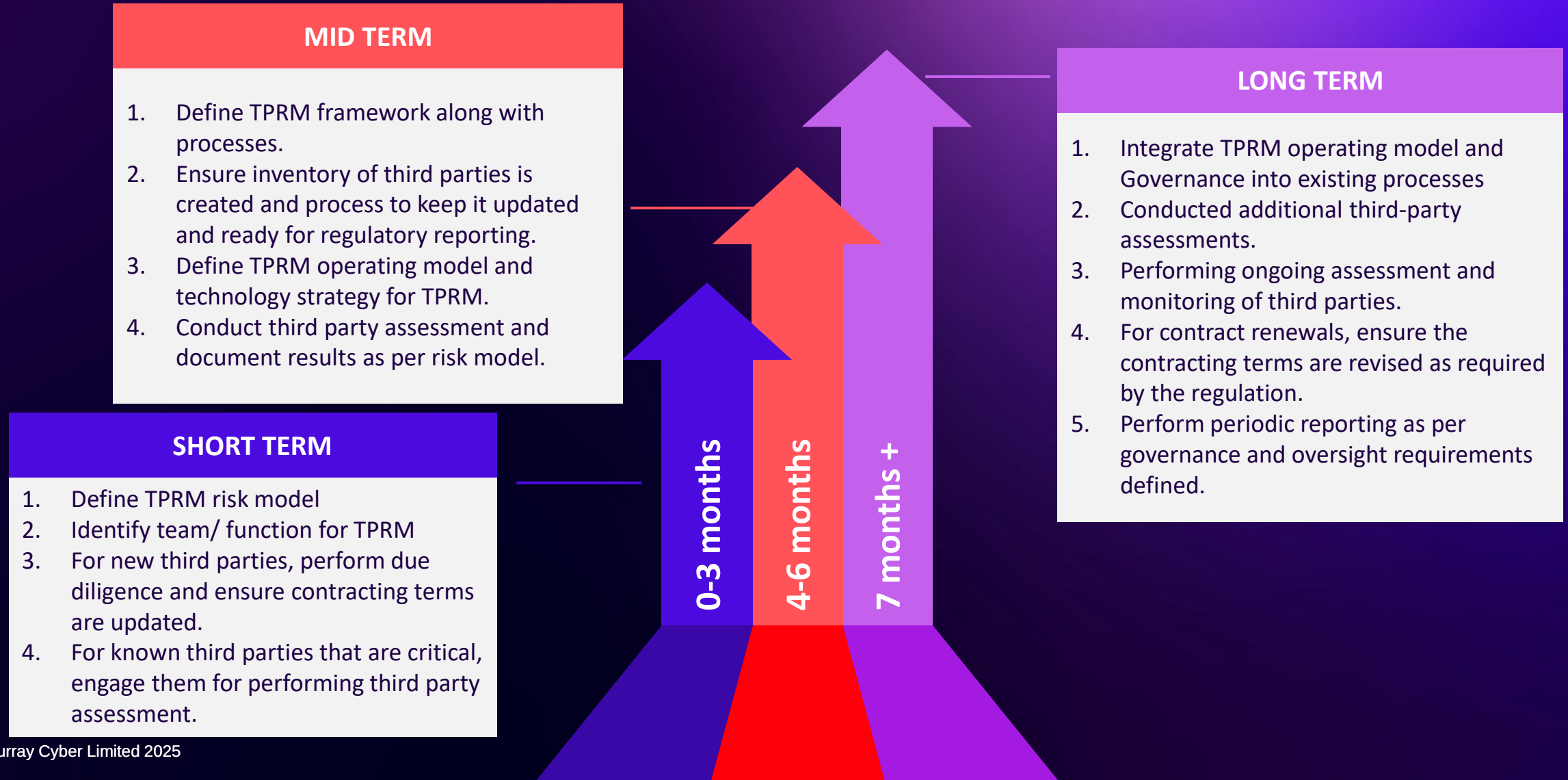
Integrating TPRM operating model and Governance into existing processes.

Manual processes which lead to inefficiencies when managing many third parties.

Translation of assessment output to risk and remediation prioritisation.



Key recommendation for operationalising TPRM framework



Thank You



Thomas
Murray

Cyber Risk

For more information:

Edward Starkie

estarkie@thomasmurray.com

Shreeji Doshi

sdoshi@thomasmurray.com