Cyber 2027: 10 key moves to elevate your cybersecurity game

WAVESTONE

Cyber Insight Day 2024

Gérôme BILLOIS
Partner
gerome.billois@wavestone.com

Matthieu GARIN
Partner
matthieu.garin@wavestone.com

Let's state the obvious

the *cybersecurity landscape* will constantly uncover

NEW CHALLENGES

2024

Compliance Boom
CRA, DORA, NIS2, AI ACT

Digital skills challenges

Geopolitical tensions

Economic uncertainties

Disruptive technologies

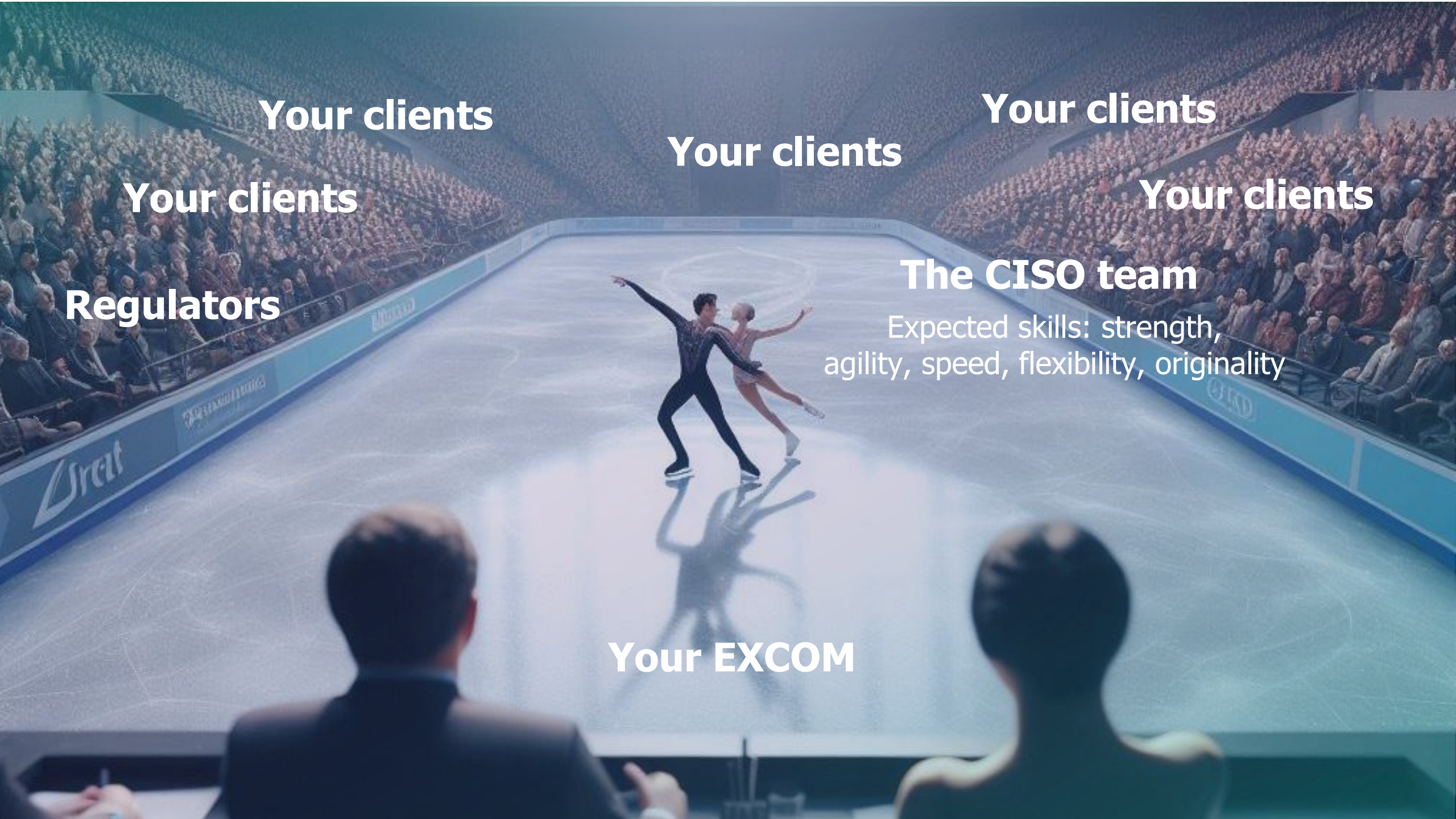
Clients' expectations

More professional cybercriminals

Cyber fatigue

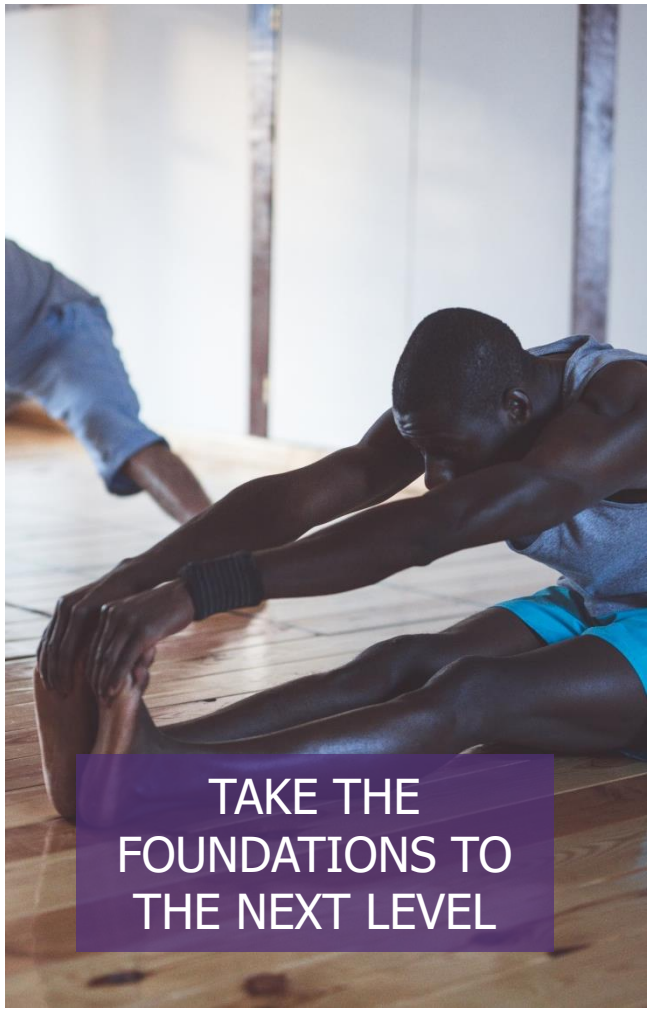
2027

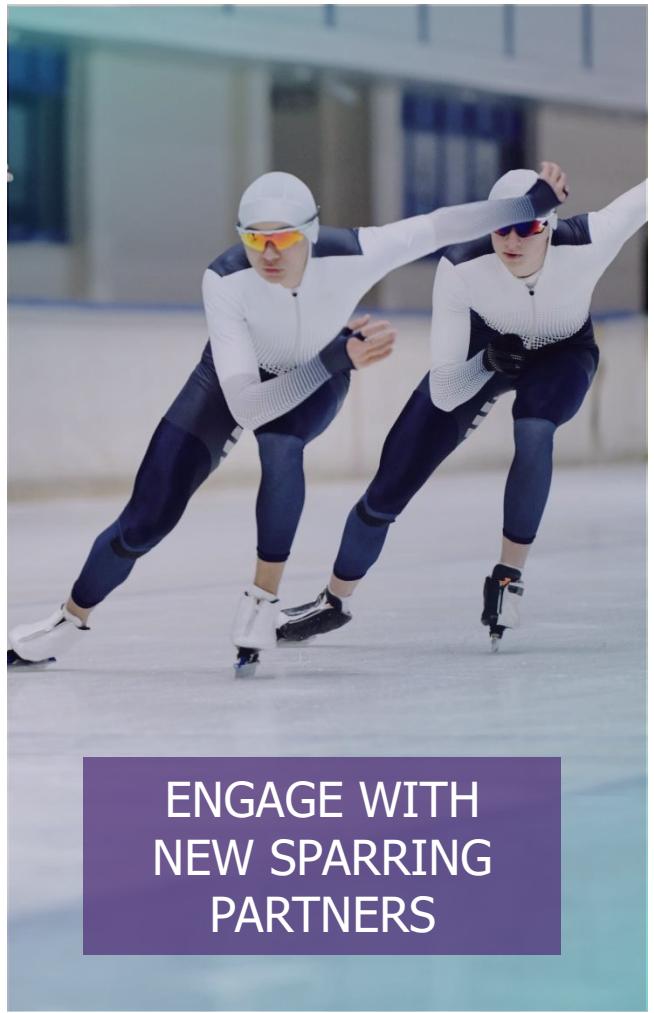
To face this ever-changing environment, CISO need to develop multiple skills: strength, agility, speed, flexibility, originality

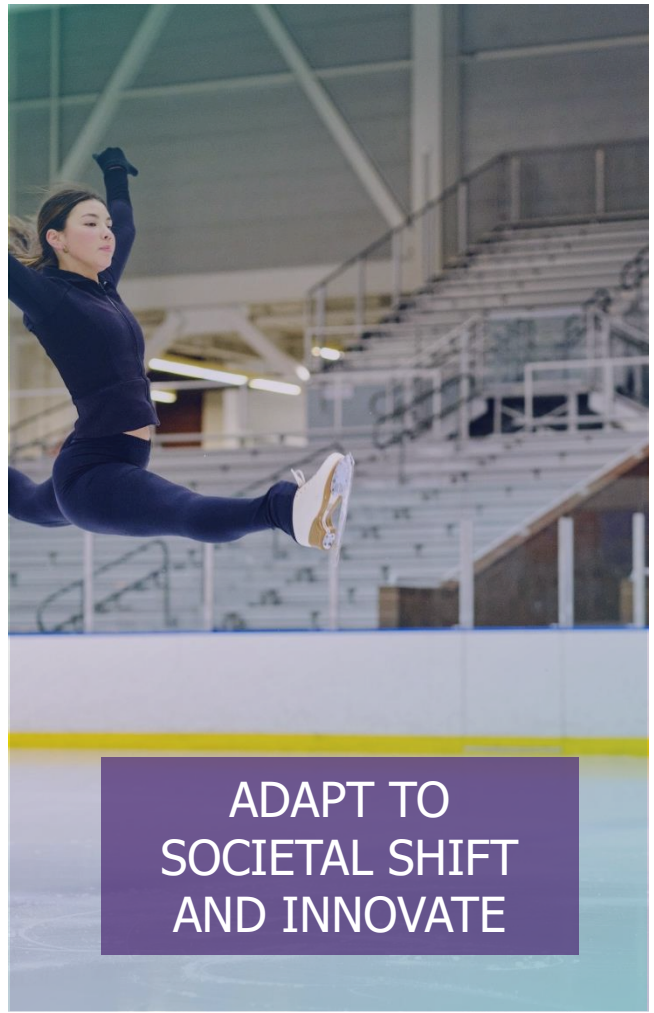

Your clients
Your clients
Your clients
Your clients
Your clients
Regulators
The CISO team
Expected skills: strength,
agility, speed, flexibility, originality
Your EXCOM

+20 CLIENTS' STRATEGIES analysed…

10 *key moves*







Cloud Security

Zero-Trust

Culture Change

TAKE THE FOUNDATIONS TO THE NEXT LEVEL

Turn

Cloud Security

into Business as usual

Shift to run mode

Ensure your basics are strong

- Make security a **priority in infrastructure projects** with a *secure-by-design* approach
- **Break down silos** between the security team and the cloud center of excellence with an agile delivery approach

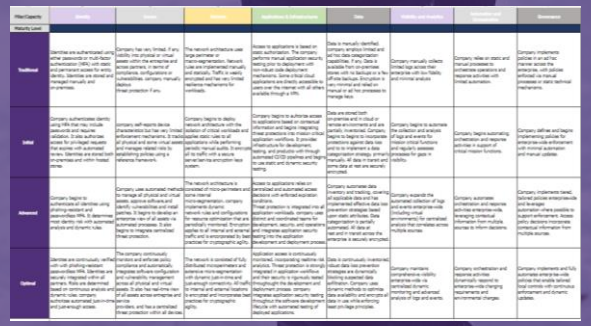
Leverage security advantages

Automate and measure

- Facilitate **seamless scaling** through the **CI/CD** automation chain and employee upskilling
- **Improve efficiency** with continuous control and agile methods
- **Adopt new strategies**: "no admin" approach in collaboration with your CTO, deceptive security…

Zero-Trust:

Beyond the philosophy, now we know what to do



Source: Wavestone Zero-Trust Maturity Assessment (based on CISA maturity assessment v2)

Identity, Device, Network, Applications & Infrastructures, Data

Visibility & Analytics, Automation & Orchestration, Governance

76 topics, **4** Maturity levels

Zero-Trust specific projects

- Zero-Trust Access
- Micro-segmentation

an obvious target but an *incremental journey*

Build for the future: adopt a convergence approach

Monitor and demonstrate convergence towards Zero-Trust through dedicated KPIs

1. **% of critical applications managed with conditional access**
2. **% users covered by Zero-Trust Access principles**
3. **% of applications covered by entitlements management**
4. **% of critical environments covered by micro-segmentation**
5. **Number of criteria to assess the level of trust**

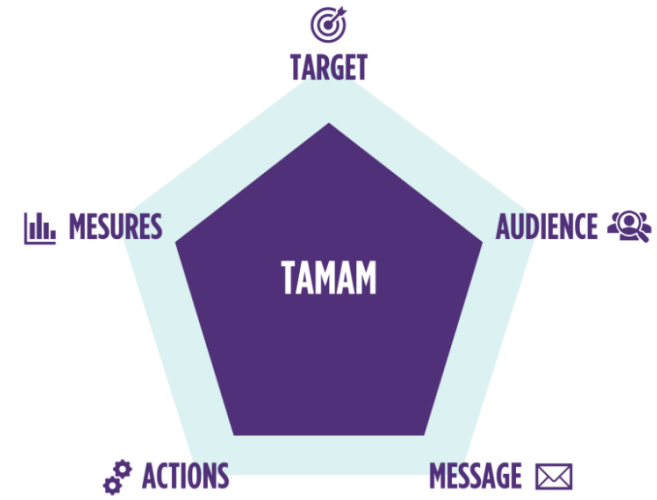
...

and ensure all new projects are **compatible** with Zero-Trust

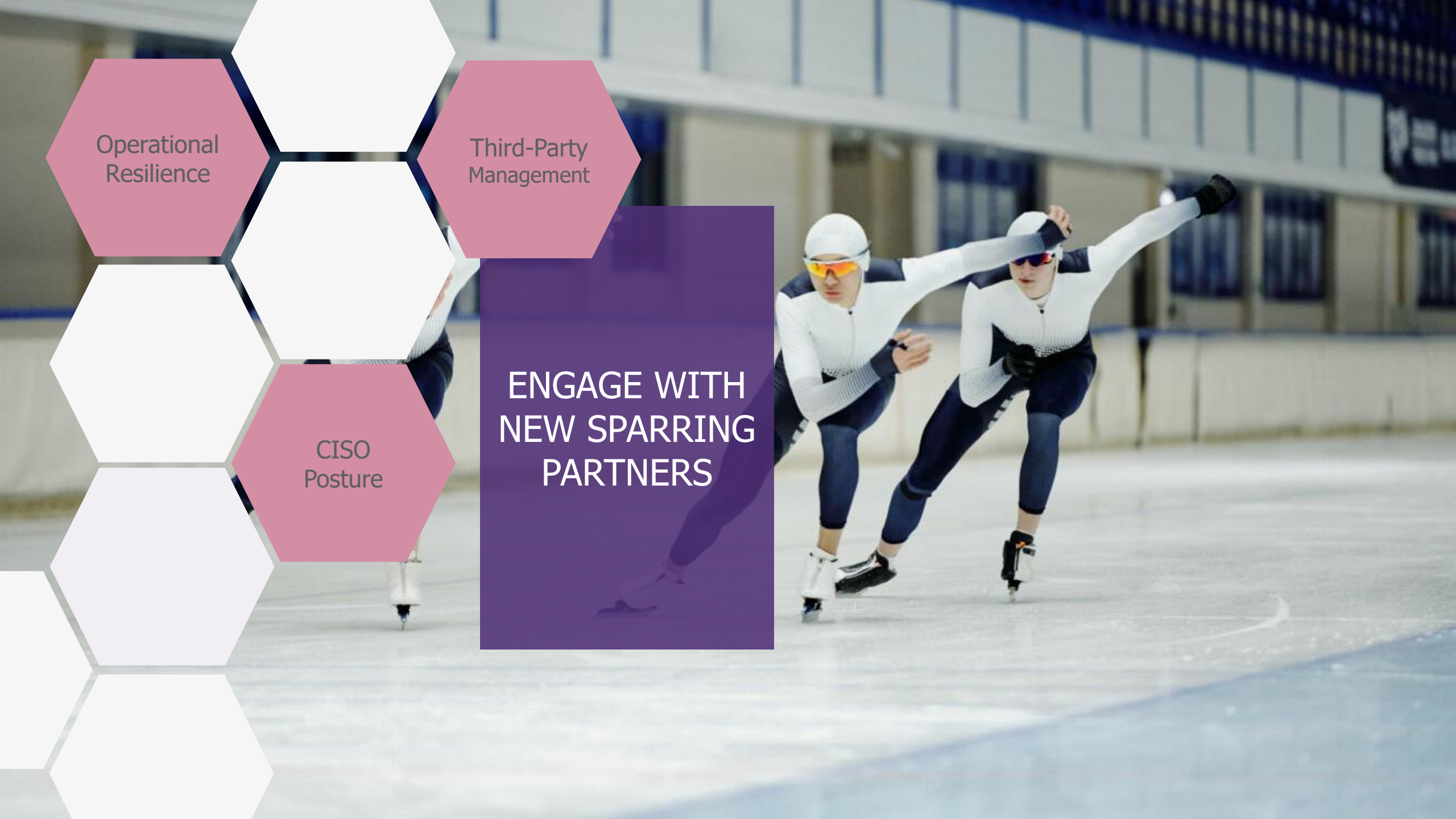
Move from awareness *to culture change*

To move towards **targeted behavioural change:**

1. **Engage** with ***local populations*** to understand practices and **identify** ***risk areas*** to target
2. **Collaborate** with them to develop ***tailored messages & solutions*** for each audience
3. **Be creative** with the ***actions*** in the program & prioritise **guilt-free approaches**
4. **Measure the** ***program's impact*** on behaviour, **highlight** ***best practices*** to empower employees and **share your** ***successes*** with your clients

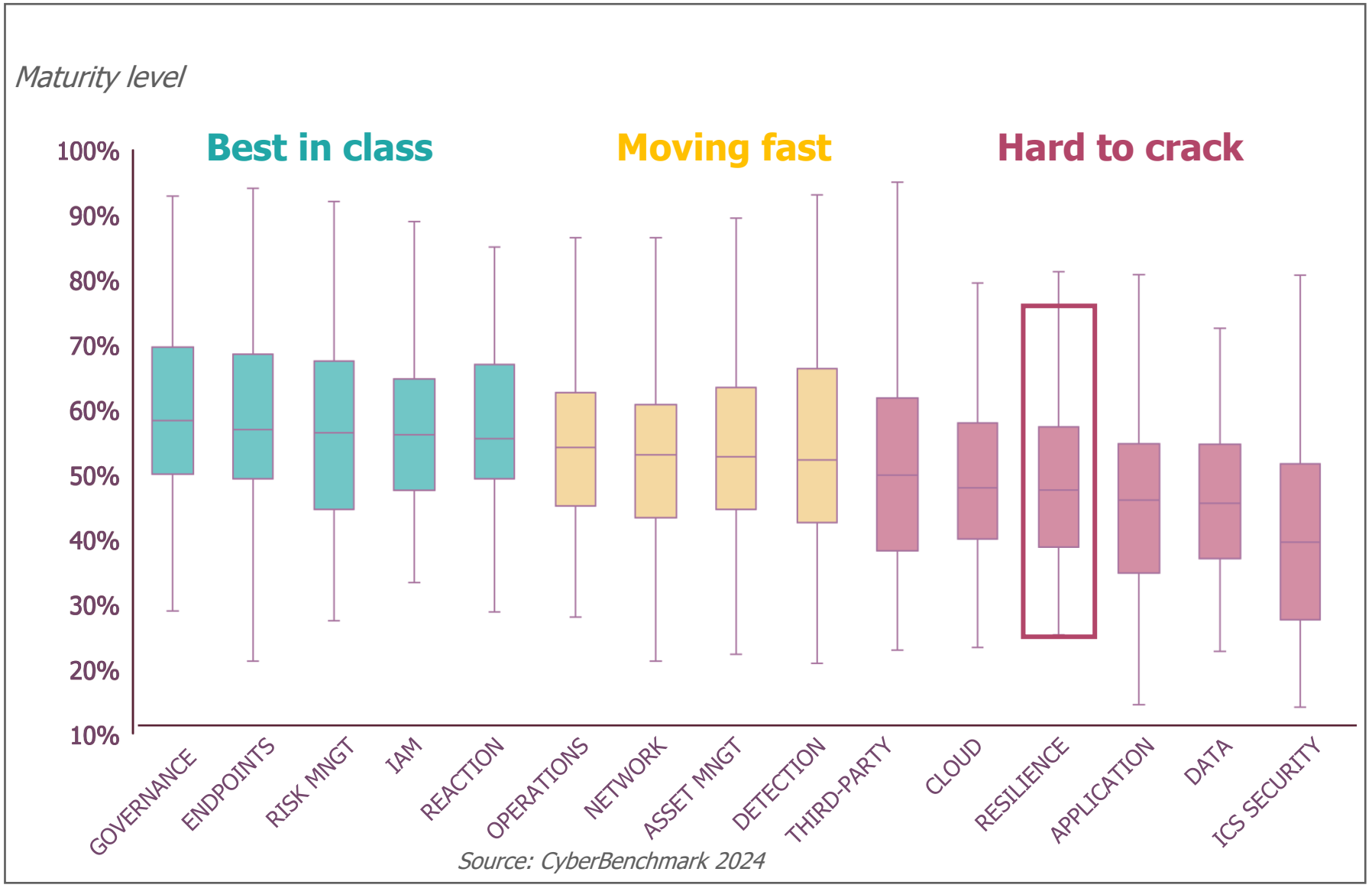


Source: Wavestone TAMAM framework


Operational Resilience
Third-Party Management
CISO Posture
ENGAGE WITH NEW SPARRING PARTNERS

Operational Resilience

Despite **regulation-driven investments** and substantial infrastructure efforts, the overall **maturity level is increasing** but **key challenges remain**



Source: CyberBenchmark 2024

Of the organisations in our benchmark:

41% Have mapped their **critical value chains** and underlying assets

65% Perform **regular tests of their backups** in accordance with their backup strategy

62% Conduct **crisis management exercises**

Operational Resilience

Onboard business to ensure the resilience of your **Minimum Viable Company**

1 **Identify** your ***minimum viable company***

Approx. 10 to 15% of business chains

2 **Define** impact ***tolerance*** with the business

Using empirical data on the impact over time

"We must settle 80% of payments intraday"

"We must deliver our product to all vulnerable customers intraday and within 3 days for non-vulnerable ones"

3 **Map** ***value chains*** and underlying assets

IT, third-parties, users and admins

4 **Identify** and assess your ***"red-zone" scenarios***

Ransomware, third-party outage, fraud…

COO sponsorship

The control action plan - along with its testing plan - will bring together cyber, IT and Business actions

Avoid Part of attack techniques that can be detected and/or mitigated

Recover Time required to rebuild key assets

Maintain Part of business activities that are operational during attack

Third party *empower*

On all fronts

Empower: create a third-party evaluation platform **accessible to everyone** in the company and promote it internally

(and if you can, build a dedicated team to track your third parties!)

Learn how to manage a **crisis with your third parties**

Contribute to ecosystem resilience

Identify non-substitutable third-party providers and set-up industry groups to work on resilience strategies and influence regulators

The CISO needs to embrace a larger scale perspective

Extending scope of responsibility

Increased Accountability

Managerial & technological expectations

CISO is dead, long live to…

The CSO in Finance

Expand your responsibilities to other teams (antifraud, physical security, resilience…) to ensure **improved coverage of the risks**

Make it concrete with a Fusion Center

A broader CISO in Industry

Bring **industrial & product security under one roof** to optimize security level and increase trust for your clients

Get ready for the **compliance boom** (Cyber Resilience Act, White House Cyber Trust Mark)

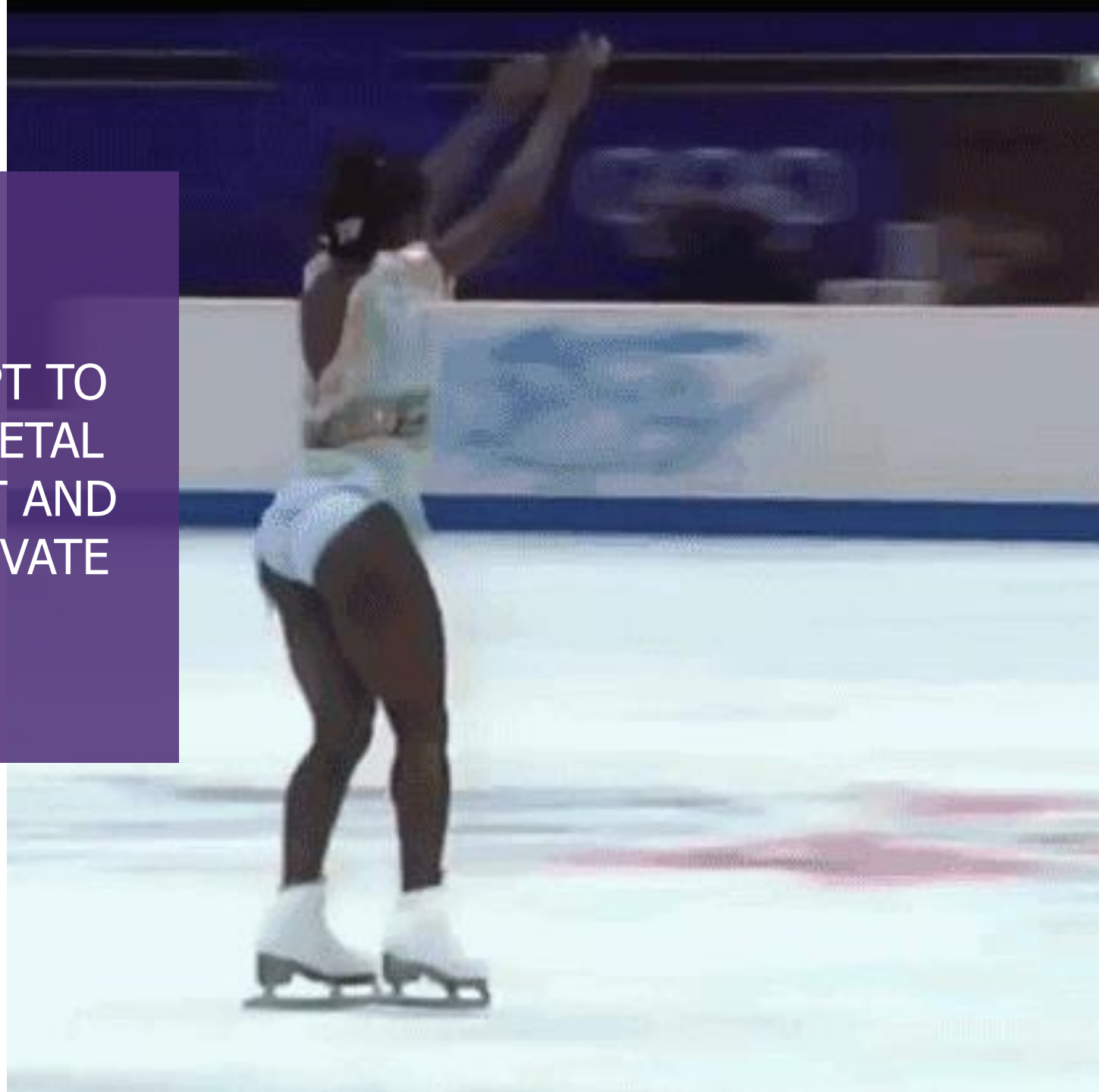
Leverage the organization to make cybersecurity a **market differentiator**

Next Gen encryption and quantum computing

AI

Decoupling

ADAPT TO SOCIETAL SHIFT AND INNOVATE



Start with **Securing A.I.**

… *don't rush* on AI for cyber

/ Develop a method to promptly **classify AI-leveraging initiatives,** prioritising **high-risk projects**

/ Define **governance and framework** against existing standards and **future regulations** (AI Act, NIST AI framework)

/ Deploy risk analyses, training and awareness **tailored** to the specific **risks and countermeasures**

/ AI-tailored red teaming: model stealing, poisoning, oracle, illusion attacks

AI has not proven to be a game changer for cyber yet

Start by building a security data hub to prepare for what's to come

Next-Gen encryption & quantum computing

a revolution underway for pioneers

Opportunities

Meet with providers to identify new solutions to **unlock new usages**:

- **Confidential computing** (encrypted memory, encrypted processor register…)
- **Homomorphic encryption** (use data without decryption)

Threat

Quantum computing – by 2030/33

Launch project to update encryption mechanisms (3-5 years):

- **Identify sensitive data,** required encryption periods and the systems managing this data
- **Identify responsible for encryption** (provider, internal development, open source)
- **Deploy post-quantum encryption engines** and adapt encryption key storage infrastructure

If you are a *multinational company* exposed to

Geopolitical tensions

Regulations leading to digital fragmentation

…anticipate DECOUPLING

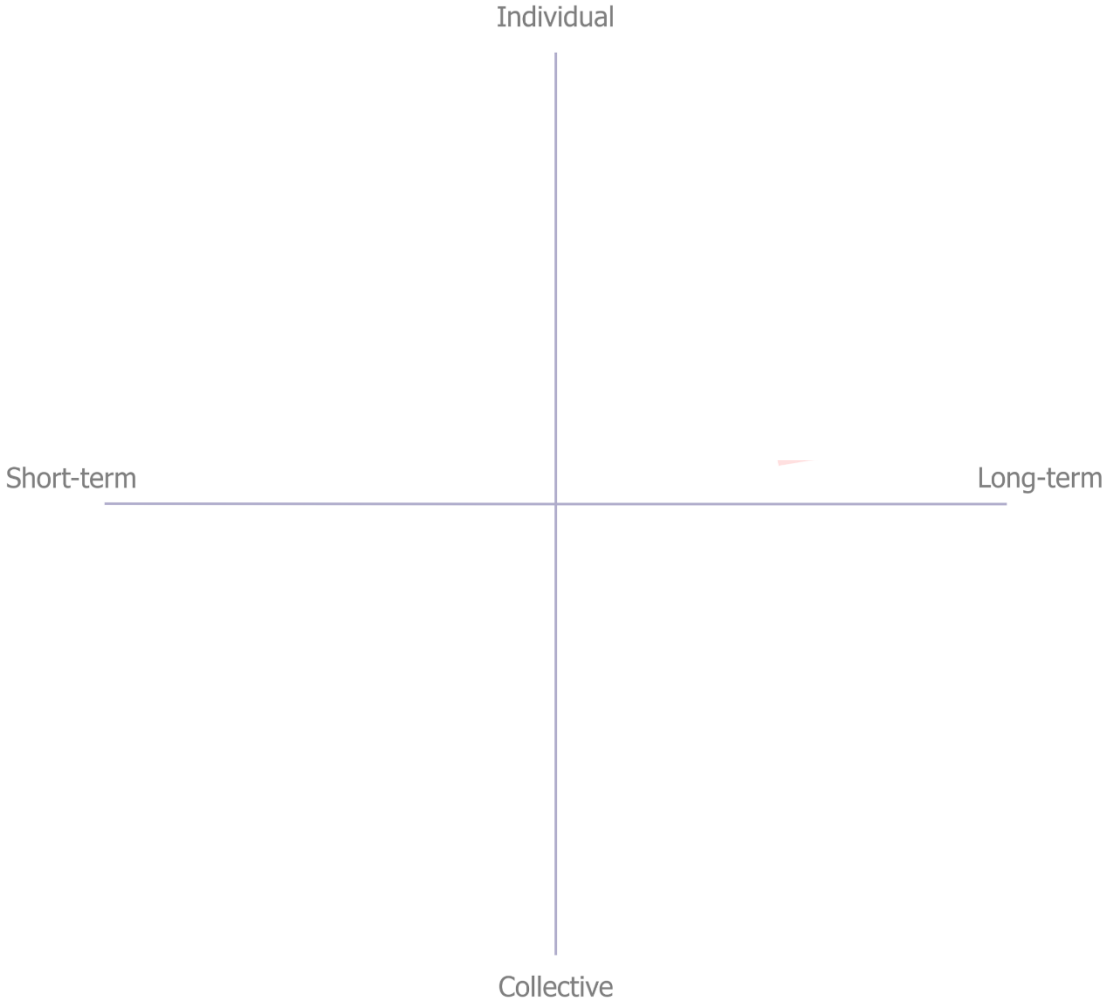
Prepare for a rapid response

- / Identify your critical geographies
- / Establish a "red-button" process: primarily for network and IAM/PAM
- / Review your crisis management procedures / What are the impacts of isolation?

Reinvent your cybersecurity architecture

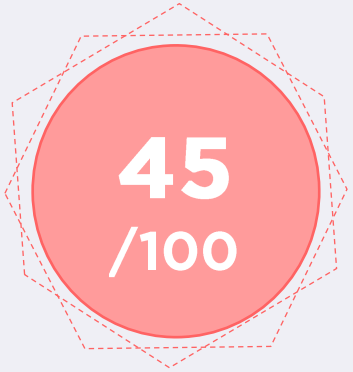
- / Build a ready-to-isolate AD architecture
- / Introduce an additional security layer between countries as necessary
- / Review your vendors' contracts and assess trustworthiness

Talent management is **a market-level issue**



Wavestone Cyber Talent Management Survey 2024 (20+ large organizations)

Overall maturity score



Focus on what you have before looking elsewhere

- *Increase* **attractiveness** *internally and promote mobility*
- *Work on* **nurturing talent retention**

How to go from a LIST OF PROJECTS...

...to a well-crafted

STRATEGY?

How to go from a LIST OF PROJECTS...

...to a well-crafted

STRATEGY?

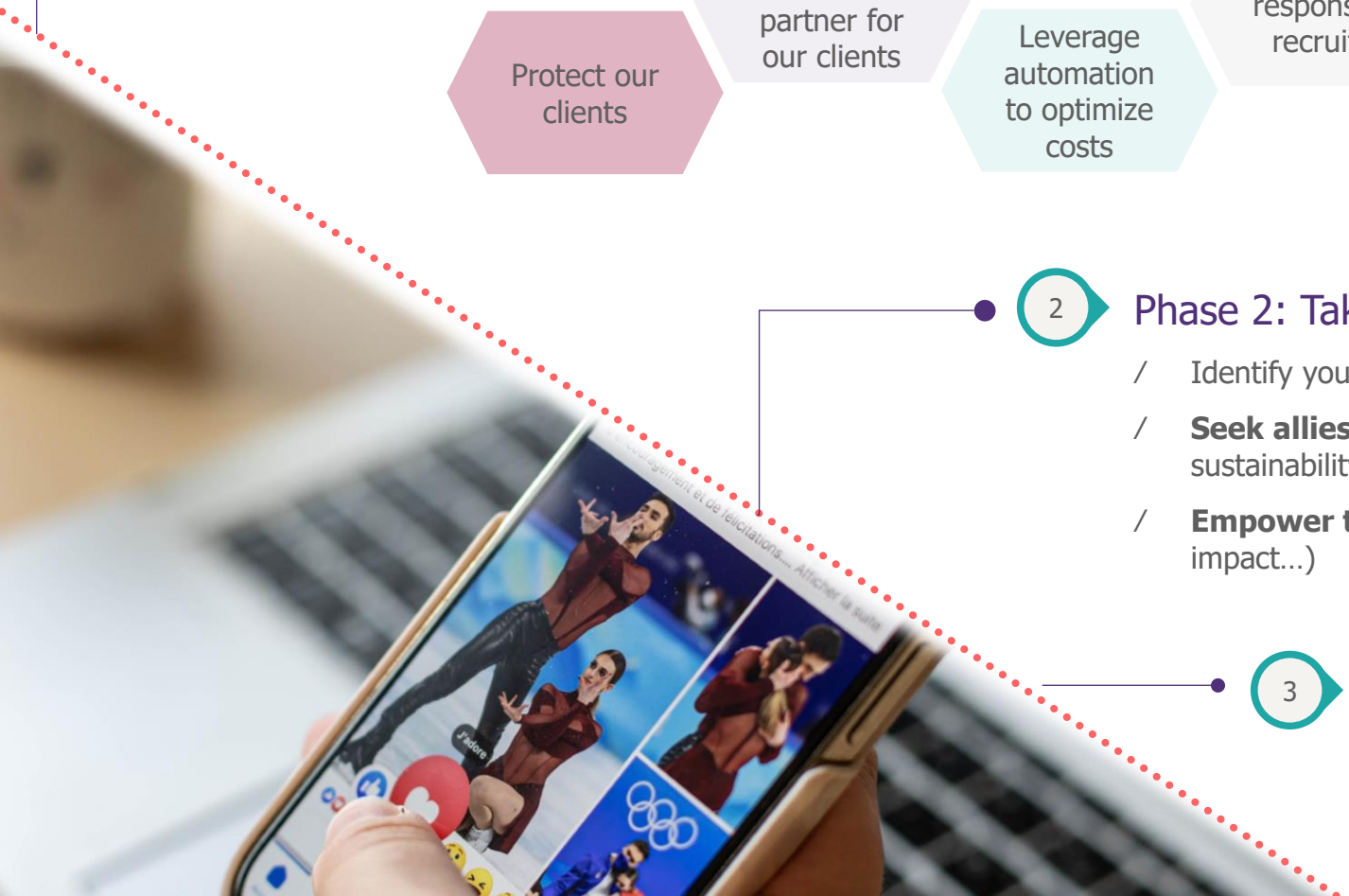
Adopt *an ambition-based* approach

1 Phase 1: Define your **ambitions**

- Maintain a top-down approach: gather your EXCOM's ambitions to **align with company strategy**
- Keep it simple: **communicate with the right level of details**

"In 2027, we will…

- Protect our clients
- Be a trusted partner for our clients
- Unlock the potential of Zero-Trust
- Leverage automation to optimize costs
- Be a responsible recruiter

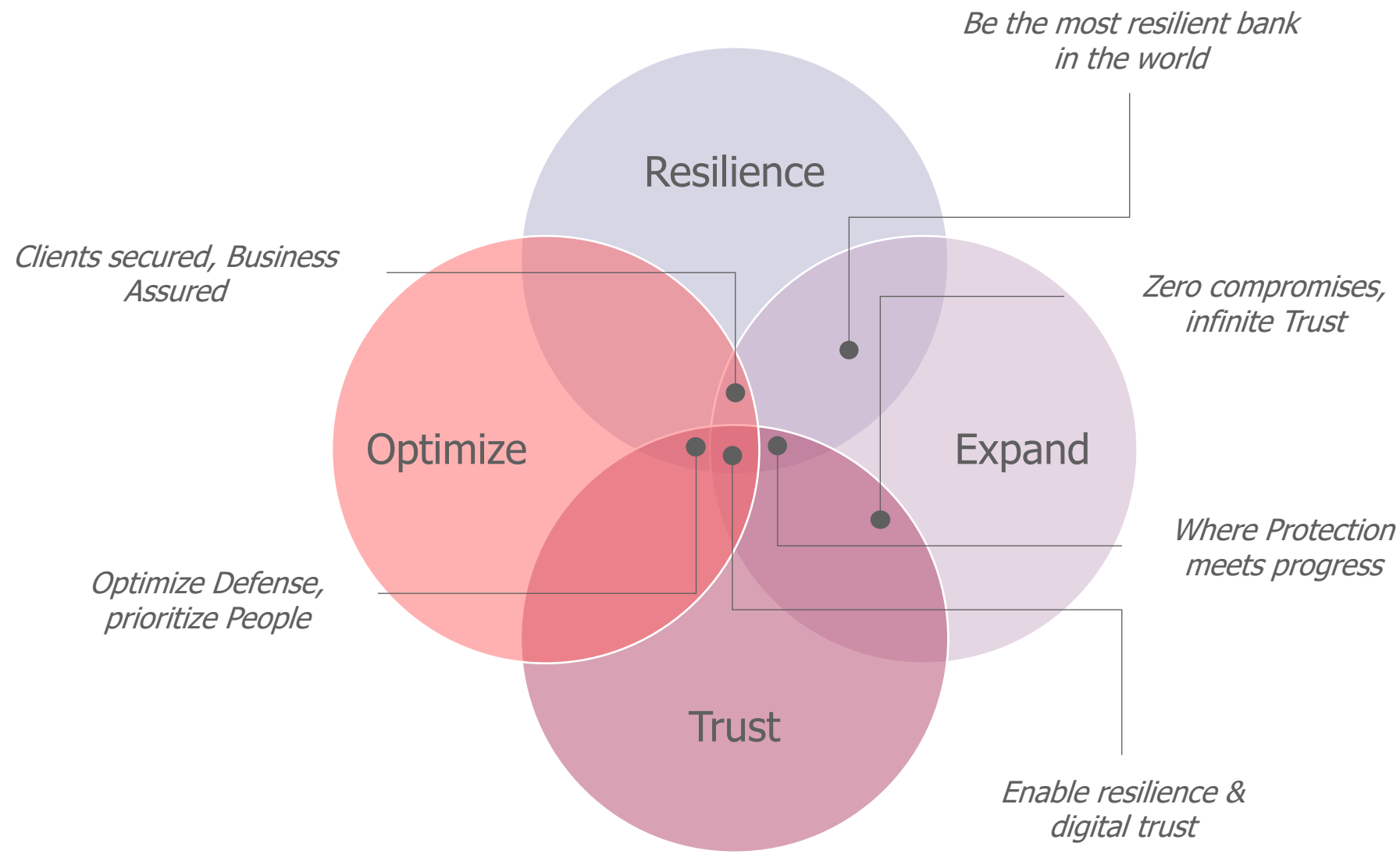


2 Phase 2: Take **actions**

- Identify your **initiatives owners** to deliver: 1 ambition = 1 owner
- **Seek allies** for each ambition and build a network of trusted actors: IT, sustainability, supply chain, purchasing, financial and HR
- **Empower the Group** on Build and Run (projects to launch, BAU KPIs, governance impact…)

3 Phase 3: Market, market, market

Market your strategy: chose your *key message and your posture*



Any questions?

Gérôme BILLOIS
Partner
gerome.billois@wavestone.com

Matthieu GARIN
Partner
matthieu.garin@wavestone.com

contact@wavestone.com