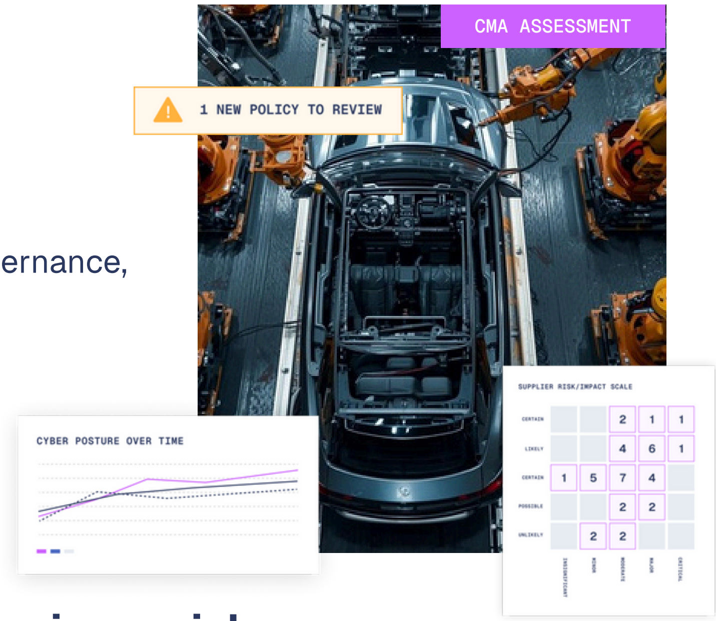
Cyber Maturity Assessment | CMA

- ✓ An in depth review of your cyber posture, governance, resilience, and incident response capabilities
- ✓ Understand your organisation's true ability to protect its data, IP, and people
- ✓ Your CMA will be conducted by an experienced CISO level consultant



SUPPLIER RISK/IMPACT SCALE

CERTAIN			2	1	1
LIKELY			4	6	1
CERTAIN	1	5	7	4	
POSSIBLE			2	2	
UNLIKELY		2	2		
	INSIGNIFICANT	MINOR	MODERATE	MAJOR	CRITICAL

In today's landscape cyber risk is business risk

Yet many organisations are still making decisions with incomplete visibility, inconsistent controls, and poor intelligence. Our CMA provides a practical, evidence-based picture of how well your organisation is managing perhaps the greatest risk modern businesses face.

The benefits of a Vambrace Cyber Maturity Assessment

- The goal of every Vambrace CMA is to help the board protect the bottom line for the next financial year and beyond.
- Not every security gap can be closed and vulnerability remediated. A CMA lets you know which are the most critical, so you can allocate resources accordingly.
- Our scoring criteria is informed by industry averages and best practices, allowing for meaningful comparisons to industry and compliance standards.

Provide insight to executive teams and aid decision making through concise, risk-focused briefings.

Assist security leaders who are planning budgets or justifying investments.

Help IT teams who are preparing for audit, regulatory review, or third-party due diligence.

Empower organisations who are scaling quickly with repeatable, reliable security.

For a clearer view of cybersecurity

Click here to start your journey

The Vambrace Cyber Maturity Assessment Framework

A CMA can cover the entire organisation or specific departments or locations. We use an easy to understand five-level maturity framework that's easy to digest and communicate across different teams. It also maps to key standards like NIST CSF, ISO 27001 and SOC2, helping to align to key compliance requirements.

Only ad hoc or reactive security practices are in place

- Controls are largely informal, undocumented, and dependent on manual processes
- Limited accountability or measurement
- Security incidents handled on a case-by-case basis without consistent documentation

1

Basic processes exist, but are inconsistently applied and often reactive

- Controls that are in place have not been adopted across the whole organisation
- Security tasks are performed regularly but not tracked or validated across the environment
- There is a lack of experienced governance, risk, and compliance leadership

2

Policies and procedures are standardised, documented, and repeatable

- Clear evidence of reviews into access controls and privileges
- Regular scanning in place with tracked remediation
- Compliance with key information security frameworks can be evidenced

3

Processes are proactive, measured, and integrated into business management

- Data and metrics drive continuous risk reduction and accountability
- Experienced CISO level led governance is in place
- Incident trends are tracked over time and lessons learned incorporated into security posture

4

Security is embedded into the organisations DNA

- Strong evidence of continuous improvement
- Automation is used effectively to accelerate tasks, reduce error, and enhance human expertise
- Intelligence driven decision making with reliable, up-to-date, and accurate data is the norm

5