Holistic Security Maturity Assessment Service

The Clarity Factory Holistic Security Maturity Model provides a framework for security leaders to assess the maturity of the partnership between physical and cyber security. It is organisational model agnostic, so can be implemented regardless of where physical and cyber security sit on the org chart.

The Clarity Factory works with clients to help you:

- Assess the maturity of the partnership in your company.
- Agree the optimal maturity, given your risk profile and appetite and current business context.
- Identify short- and medium-term priorities to enhance the partnership for the benefit of business opportunities and operational resilience.
- Develop a forward workplan to optimise the partnership to drive competitive advantage for your company.

We work with either the physical or cyber security team, or both teams together, depending on your preference.

Holistic Security Maturity Self-Assessment tool licensing and report

- Individual and team access to Holistic Security Maturity self-assessment tool.
- Individual self-assessment scorecards and overall team scorecard with high-level feedback and observations.
- 1-hour call with Rachel Briggs to review scores and discuss feedback and suggested next steps.

Holistic Security Self-Assessment Workshop

- Access to self-assessment tool.
- Individual and team scorecards, as above.
- Half-day workshop facilitated by The Clarity Factory.

Holistic Security Independent Assessment and Workshop

- Access to self-assessment tool.
- Individual and team scorecards.
- Clarity Factory independent maturity assessment, using proprietary framework and data, interviews with physical and cyber security teams and other key company stakeholders.
- Independent maturity assessment report, providing Holistic Security Maturity score, areas of strength, opportunities for development, and suggested priority next steps.
- Half-day workshop to review results of assessment, interrogate key challenges and opportunities, and identify short- and medium-term priorities.

THE PRACTICALITIES

Our Holistic Security Maturity Assessment can be delivered through a self-assessment or an independent assessment.

Our workshops can be delivered in-person or virtually.

Holistic Security Self-Assessment tool licensing and report starts from £6,000.

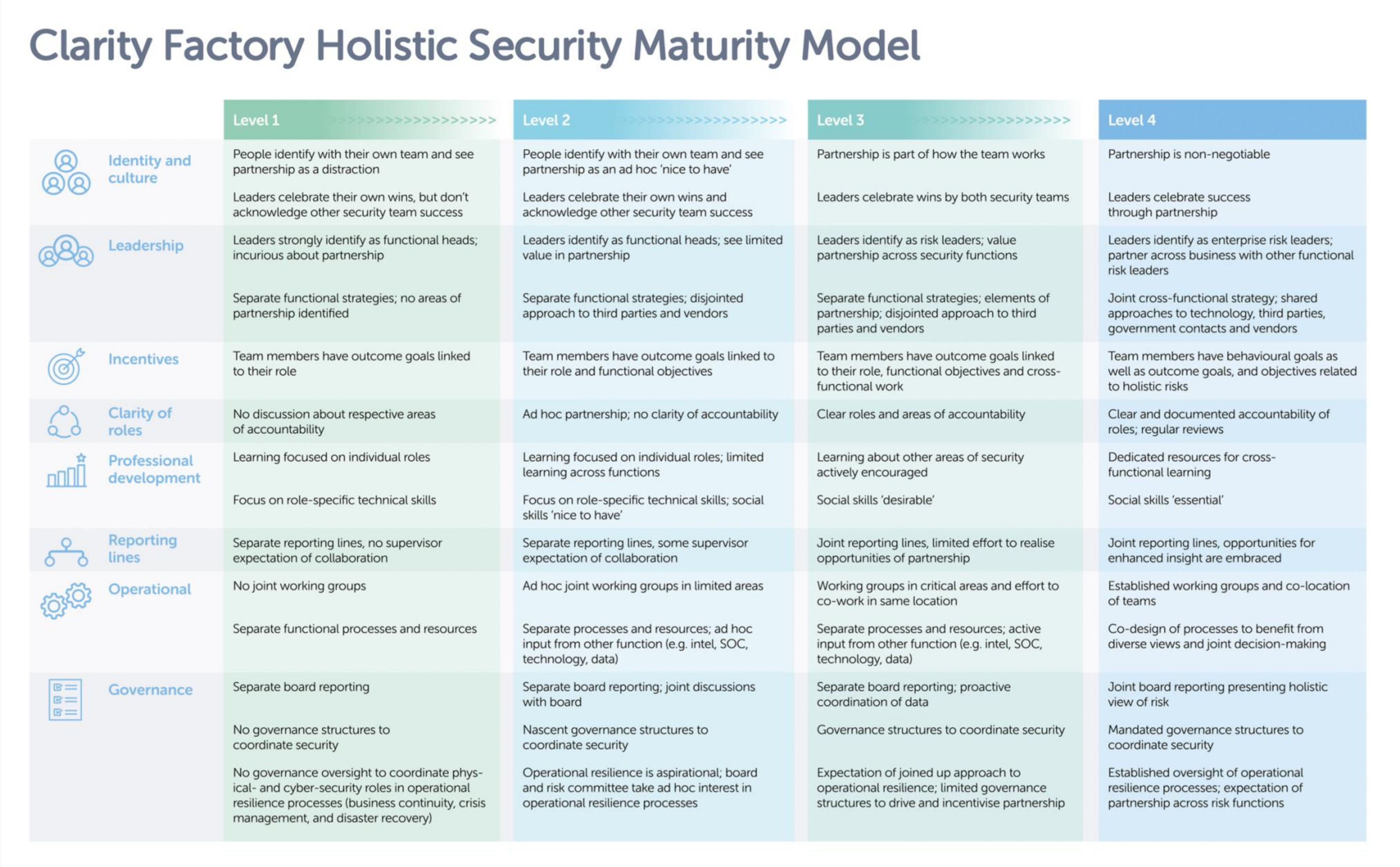
The Holistic Security Self-Assessment and Workshop starts from £10,000, plus travel and expenses.

The Holistic Security Independent Assessment and Workshop starts from £25,000, plus travel and expenses.

We are pleased to work with you to tailor the assessment to your needs.

To discuss our Holistic Security Maturity Assessment, contact

Rachel Briggs OBE
The Clarity Factory
rachel.briggs@clarityfactory.com



Clarity Factory Holistic Security Maturity Model

	Level 1	Level 2	Level 3	Level 4
Identity and culture	People identify with their own team and see partnership as a distraction Leaders celebrate their own wins, but don't acknowledge other security team success	People identify with their own team and see partnership as an ad hoc 'nice to have' Leaders celebrate their own wins and acknowledge other security team success	Partnership is part of how the team works Leaders celebrate wins by both security teams	Partnership is non-negotiable Leaders celebrate success through partnership
Leadership	Leaders strongly identify as functional heads; incurious about partnership Separate functional strategies; no areas of partnership identified	Leaders identify as functional heads; see limited value in partnership Separate functional strategies; disjointed approach to third parties and vendors	Leaders identify as risk leaders; value partnership across security functions Separate functional strategies; elements of partnership; disjointed approach to third parties and vendors	Leaders identify as enterprise risk leaders; partner across business with other functional risk leaders Joint cross-functional strategy; shared approaches to technology, third parties, government contacts and vendors
Incentives	Team members have outcome goals linked to their role	Team members have outcome goals linked to their role and functional objectives	Team members have outcome goals linked to their role, functional objectives and cross-functional work	Team members have behavioural goals as well as outcome goals, and objectives related to holistic risks
Clarity of roles	No discussion about respective areas of accountability	Ad hoc partnership; no clarity of accountability	Clear roles and areas of accountability	Clear and documented accountability of roles; regular reviews
Professional development	Learning focused on individual roles Focus on role-specific technical skills	Learning focused on individual roles; limited learning across functions Focus on role-specific technical skills; social skills 'nice to have'	Learning about other areas of security actively encouraged Social skills 'desirable'	Dedicated resources for cross-functional learning Social skills 'essential'
Reporting lines	Separate reporting lines, no supervisor expectation of collaboration	Separate reporting lines, some supervisor expectation of collaboration	Joint reporting lines, limited effort to realise opportunities of partnership	Joint reporting lines, opportunities for enhanced insight are embraced
Operational	No joint working groups Separate functional processes and resources	Ad hoc joint working groups in limited areas Separate processes and resources; ad hoc input from other function (e.g. intel, SOC, technology, data)	Working groups in critical areas and effort to co-work in same location Separate processes and resources; active input from other function (e.g. intel, SOC, technology, data)	Established working groups and co-location of teams Co-design of processes to benefit from diverse views and joint decision-making
Governance	Separate board reporting No governance structures to coordinate security No governance oversight to coordinate physical- and cyber-security roles in operational resilience processes (business continuity, crisis management, and disaster recovery)	Separate board reporting; joint discussions with board Nascent governance structures to coordinate security Operational resilience is aspirational; board and risk committee take ad hoc interest in operational resilience processes	Separate board reporting; proactive coordination of data Governance structures to coordinate security Expectation of joined up approach to operational resilience; limited governance structures to drive and incentivise partnership	Joint board reporting presenting holistic view of risk Mandated governance structures to coordinate security Established oversight of operational resilience processes; expectation of partnership across risk functions