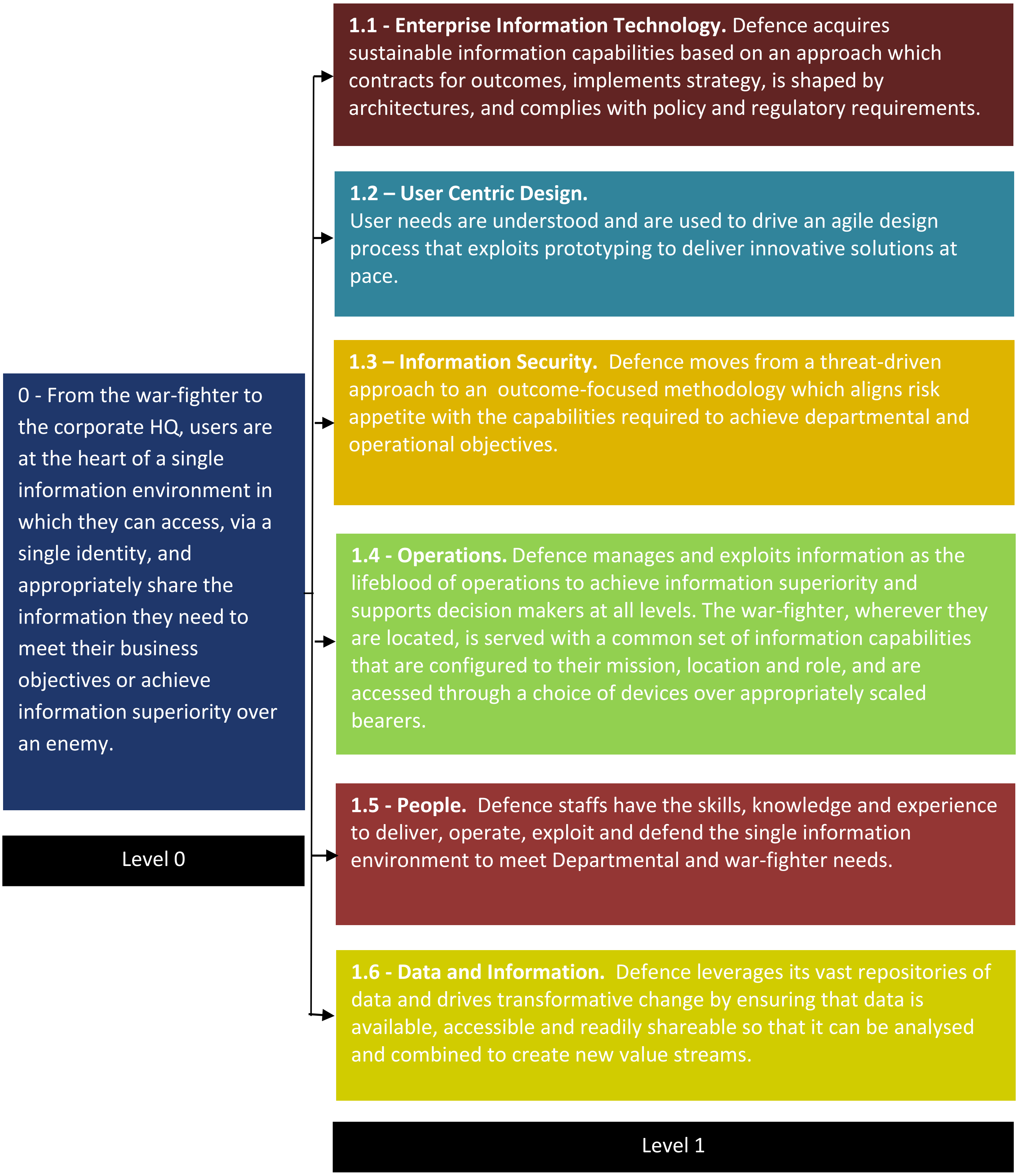
STRATEGIC OUTCOMES Enclosure 1



0 - From the war-fighter to the corporate HQ, users are at the heart of a single information environment in which they can access, via a single identity, and appropriately share the information they need to meet their business objectives or achieve information superiority over an enemy.

Level 0

1.1 - Enterprise Information Technology. Defence acquires sustainable information capabilities based on an approach which contracts for outcomes, implements strategy, is shaped by architectures, and complies with policy and regulatory requirements.

1.2 – User Centric Design.
User needs are understood and are used to drive an agile design process that exploits prototyping to deliver innovative solutions at pace.

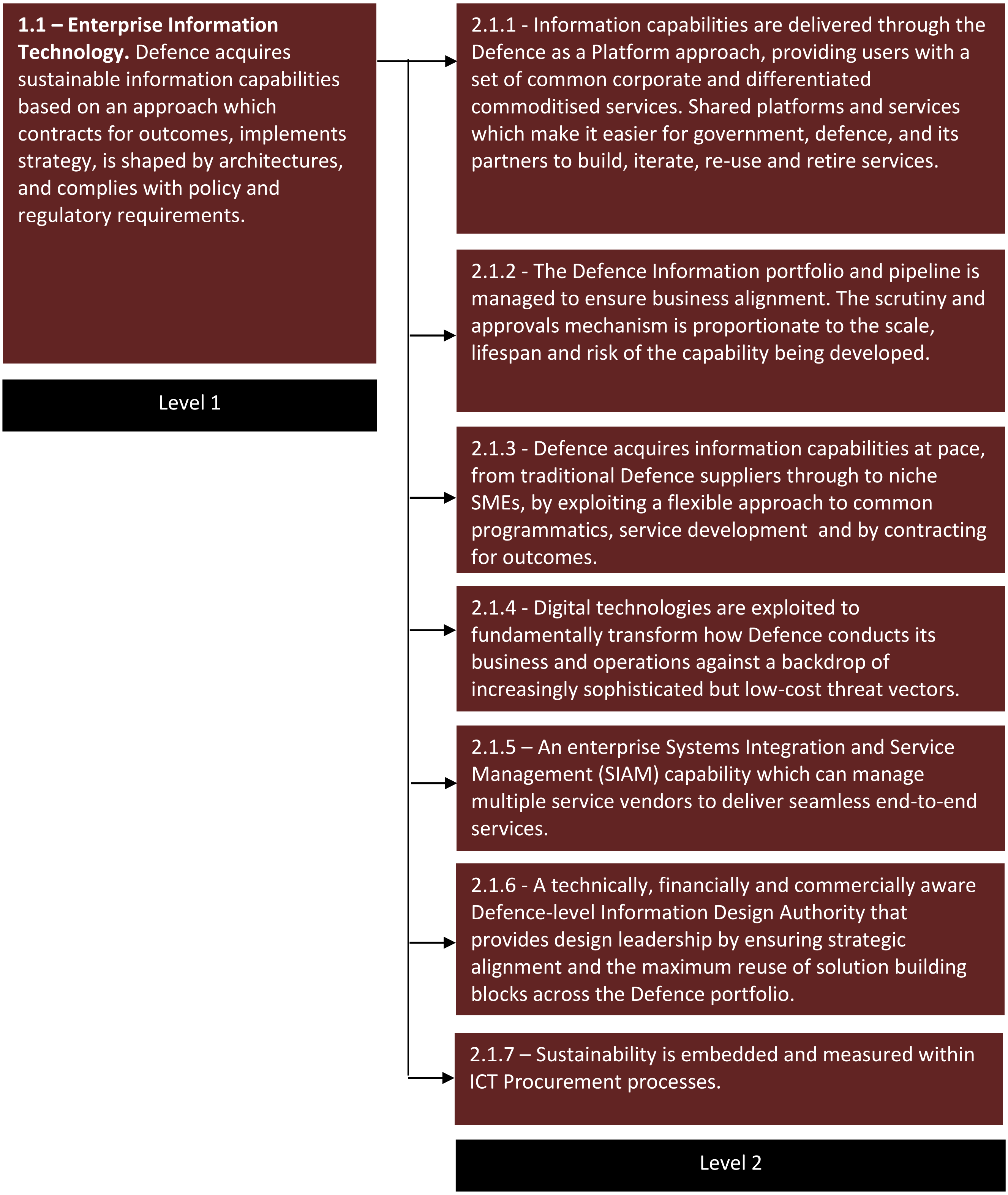
1.3 – Information Security. Defence moves from a threat-driven approach to an outcome-focused methodology which aligns risk appetite with the capabilities required to achieve departmental and operational objectives.

1.4 - Operations. Defence manages and exploits information as the lifeblood of operations to achieve information superiority and supports decision makers at all levels. The war-fighter, wherever they are located, is served with a common set of information capabilities that are configured to their mission, location and role, and are accessed through a choice of devices over appropriately scaled bearers.

1.5 - People. Defence staffs have the skills, knowledge and experience to deliver, operate, exploit and defend the single information environment to meet Departmental and war-fighter needs.

1.6 - Data and Information. Defence leverages its vast repositories of data and drives transformative change by ensuring that data is available, accessible and readily shareable so that it can be analysed and combined to create new value streams.

Level 1



1.1 – Enterprise Information Technology. Defence acquires sustainable information capabilities based on an approach which contracts for outcomes, implements strategy, is shaped by architectures, and complies with policy and regulatory requirements.

Level 1

2.1.1 - Information capabilities are delivered through the Defence as a Platform approach, providing users with a set of common corporate and differentiated commoditised services. Shared platforms and services which make it easier for government, defence, and its partners to build, iterate, re-use and retire services.

2.1.2 - The Defence Information portfolio and pipeline is managed to ensure business alignment. The scrutiny and approvals mechanism is proportionate to the scale, lifespan and risk of the capability being developed.

2.1.3 - Defence acquires information capabilities at pace, from traditional Defence suppliers through to niche SMEs, by exploiting a flexible approach to common programmatics, service development and by contracting for outcomes.

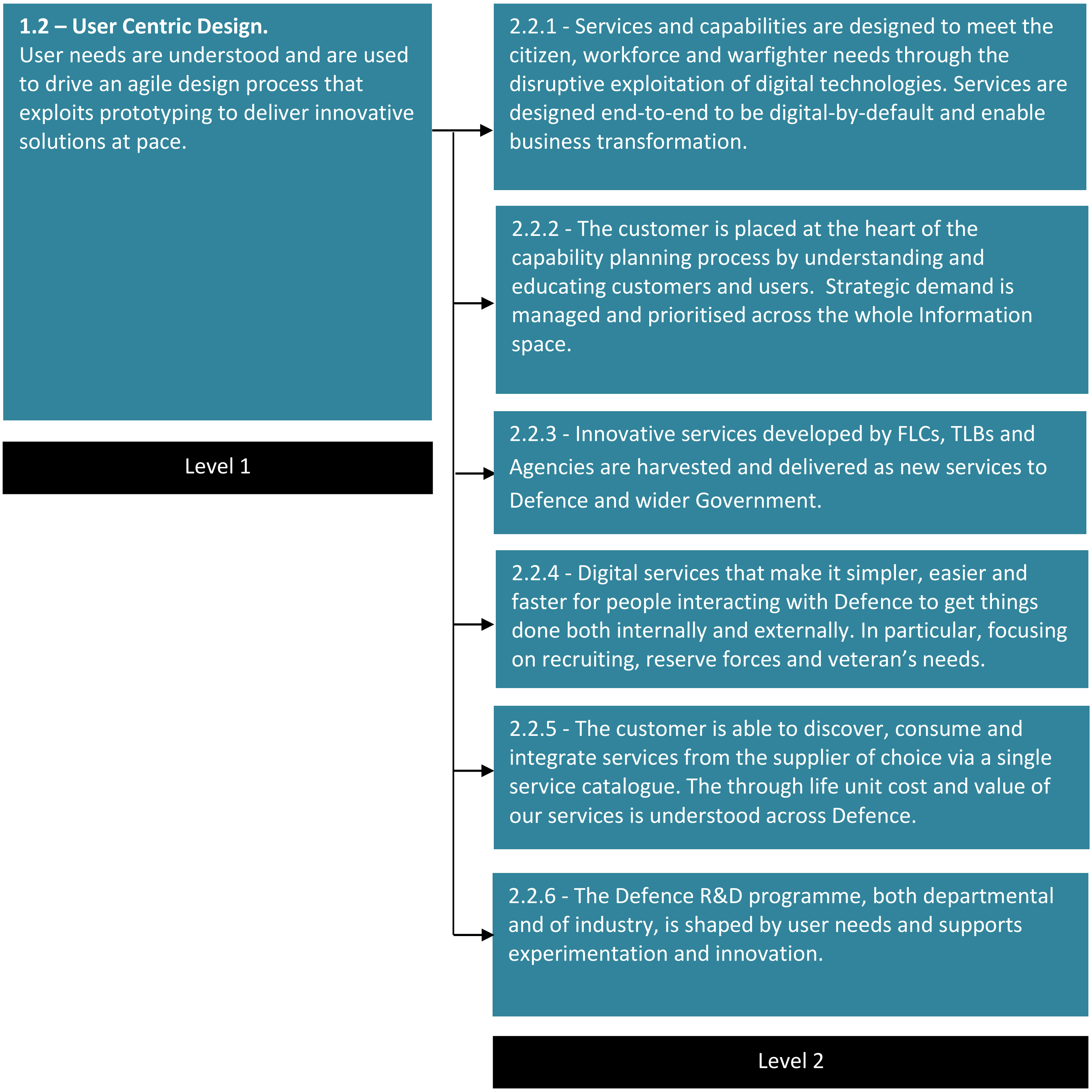
2.1.4 - Digital technologies are exploited to fundamentally transform how Defence conducts its business and operations against a backdrop of increasingly sophisticated but low-cost threat vectors.

2.1.5 – An enterprise Systems Integration and Service Management (SIAM) capability which can manage multiple service vendors to deliver seamless end-to-end services.

2.1.6 - A technically, financially and commercially aware Defence-level Information Design Authority that provides design leadership by ensuring strategic alignment and the maximum reuse of solution building blocks across the Defence portfolio.

2.1.7 – Sustainability is embedded and measured within ICT Procurement processes.

Level 2



1.2 – User Centric Design.
User needs are understood and are used to drive an agile design process that exploits prototyping to deliver innovative solutions at pace.

Level 1

2.2.1 - Services and capabilities are designed to meet the citizen, workforce and warfighter needs through the disruptive exploitation of digital technologies. Services are designed end-to-end to be digital-by-default and enable business transformation.

2.2.2 - The customer is placed at the heart of the capability planning process by understanding and educating customers and users. Strategic demand is managed and prioritised across the whole Information space.

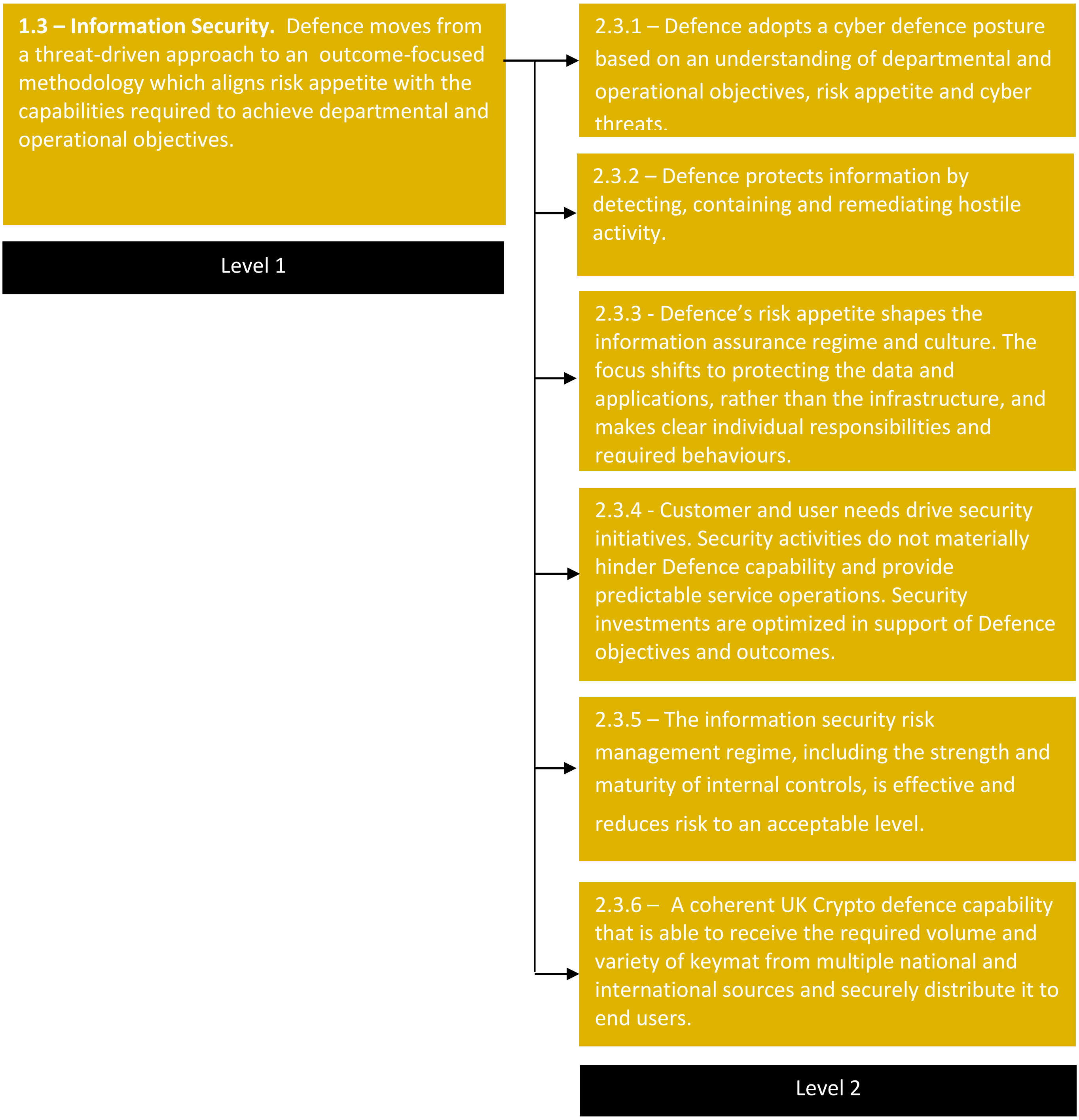
2.2.3 - Innovative services developed by FLCs, TLBs and Agencies are harvested and delivered as new services to Defence and wider Government.

2.2.4 - Digital services that make it simpler, easier and faster for people interacting with Defence to get things done both internally and externally. In particular, focusing on recruiting, reserve forces and veteran's needs.

2.2.5 - The customer is able to discover, consume and integrate services from the supplier of choice via a single service catalogue. The through life unit cost and value of our services is understood across Defence.

2.2.6 - The Defence R&D programme, both departmental and of industry, is shaped by user needs and supports experimentation and innovation.

Level 2



1.3 – Information Security. Defence moves from a threat-driven approach to an outcome-focused methodology which aligns risk appetite with the capabilities required to achieve departmental and operational objectives.

Level 1

2.3.1 – Defence adopts a cyber defence posture based on an understanding of departmental and operational objectives, risk appetite and cyber threats.

2.3.2 – Defence protects information by detecting, containing and remediating hostile activity.

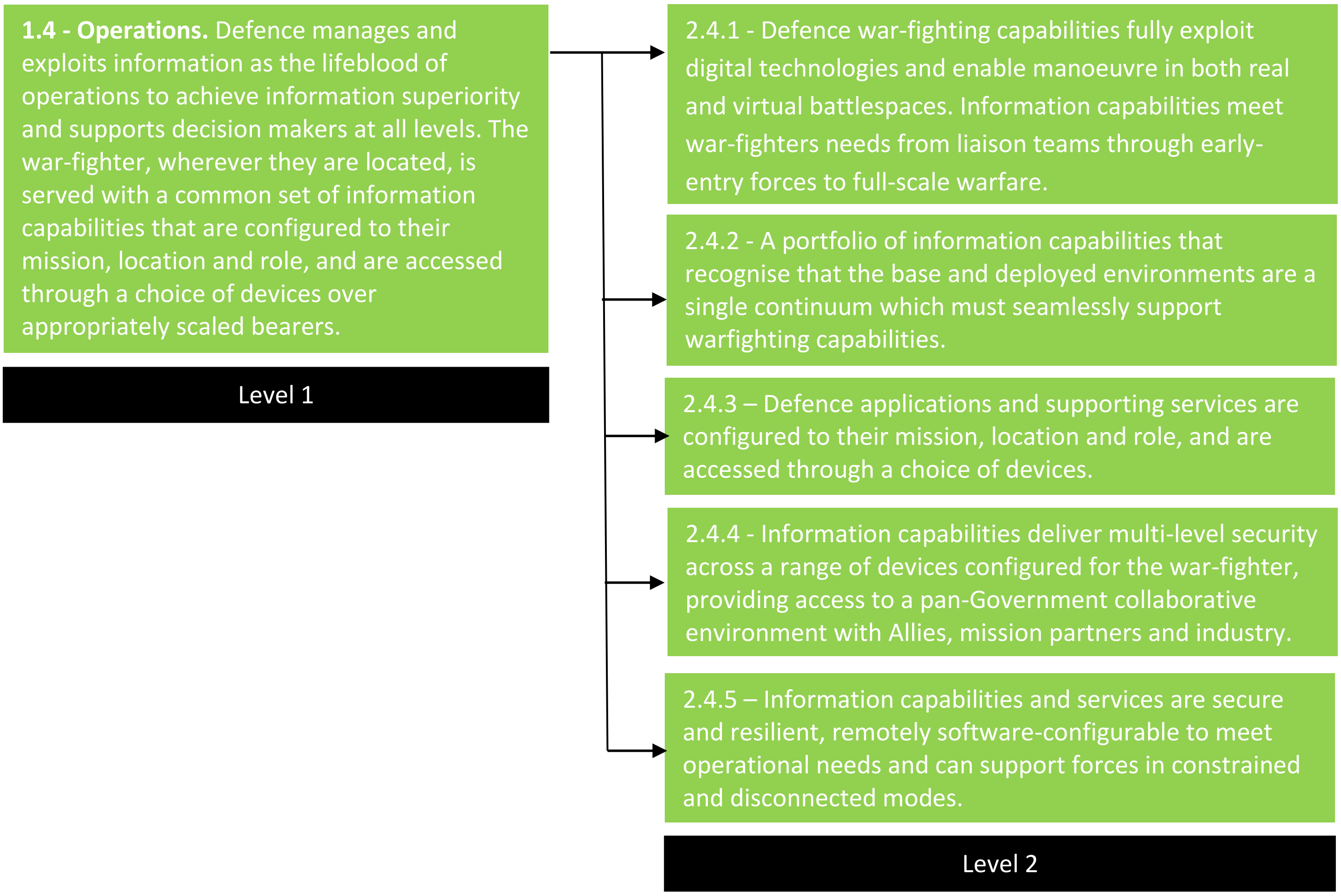
2.3.3 - Defence's risk appetite shapes the information assurance regime and culture. The focus shifts to protecting the data and applications, rather than the infrastructure, and makes clear individual responsibilities and required behaviours.

2.3.4 - Customer and user needs drive security initiatives. Security activities do not materially hinder Defence capability and provide predictable service operations. Security investments are optimized in support of Defence objectives and outcomes.

2.3.5 – The information security risk management regime, including the strength and maturity of internal controls, is effective and reduces risk to an acceptable level.

2.3.6 – A coherent UK Crypto defence capability that is able to receive the required volume and variety of keymat from multiple national and international sources and securely distribute it to end users.

Level 2



1.4 - Operations. Defence manages and exploits information as the lifeblood of operations to achieve information superiority and supports decision makers at all levels. The war-fighter, wherever they are located, is served with a common set of information capabilities that are configured to their mission, location and role, and are accessed through a choice of devices over appropriately scaled bearers.

Level 1

2.4.1 - Defence war-fighting capabilities fully exploit digital technologies and enable manoeuvre in both real and virtual battlespaces. Information capabilities meet war-fighters needs from liaison teams through early-entry forces to full-scale warfare.

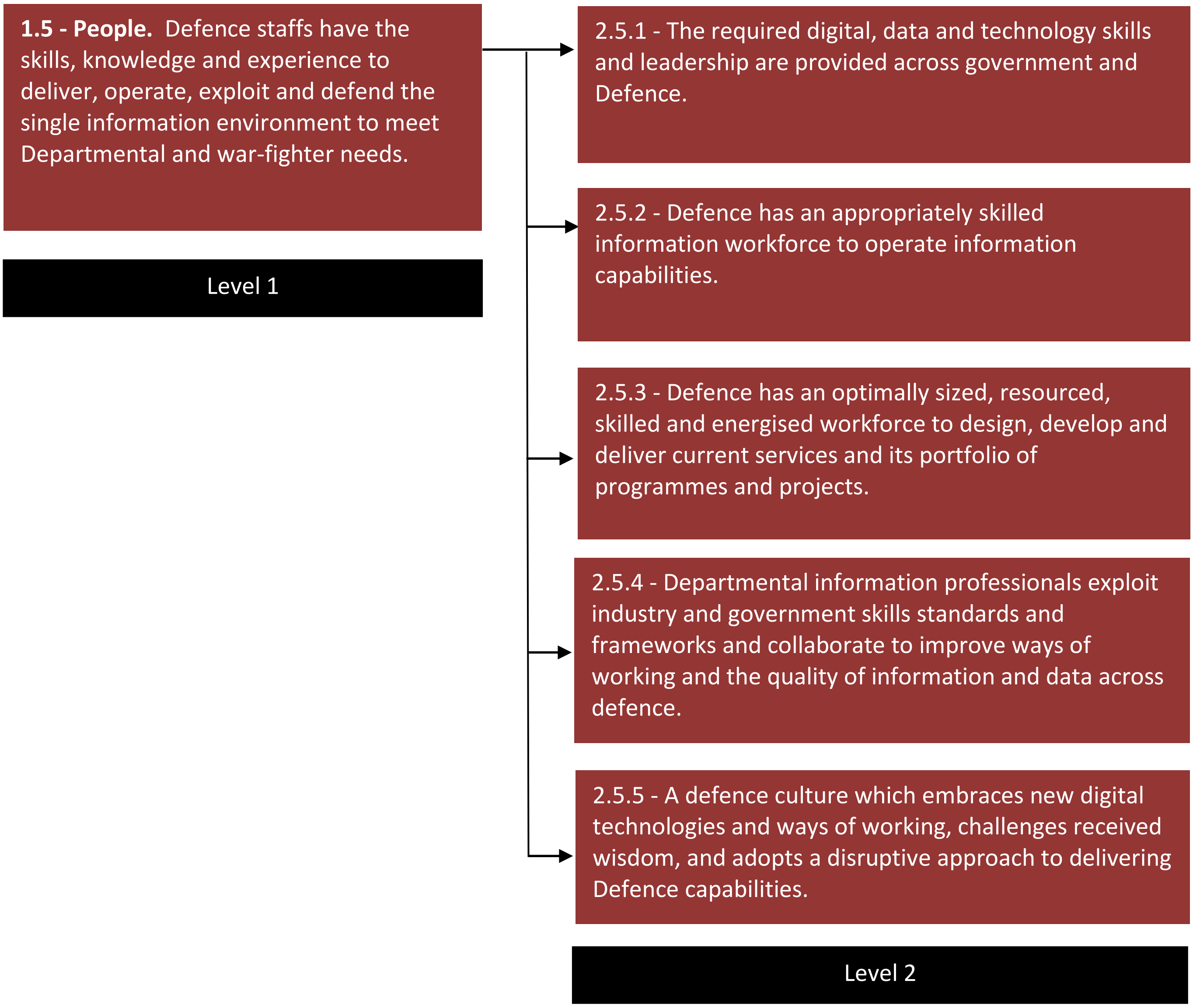
2.4.2 - A portfolio of information capabilities that recognise that the base and deployed environments are a single continuum which must seamlessly support warfighting capabilities.

2.4.3 – Defence applications and supporting services are configured to their mission, location and role, and are accessed through a choice of devices.

2.4.4 - Information capabilities deliver multi-level security across a range of devices configured for the war-fighter, providing access to a pan-Government collaborative environment with Allies, mission partners and industry.

2.4.5 – Information capabilities and services are secure and resilient, remotely software-configurable to meet operational needs and can support forces in constrained and disconnected modes.

Level 2



1.5 - People. Defence staffs have the skills, knowledge and experience to deliver, operate, exploit and defend the single information environment to meet Departmental and war-fighter needs.

Level 1

2.5.1 - The required digital, data and technology skills and leadership are provided across government and Defence.

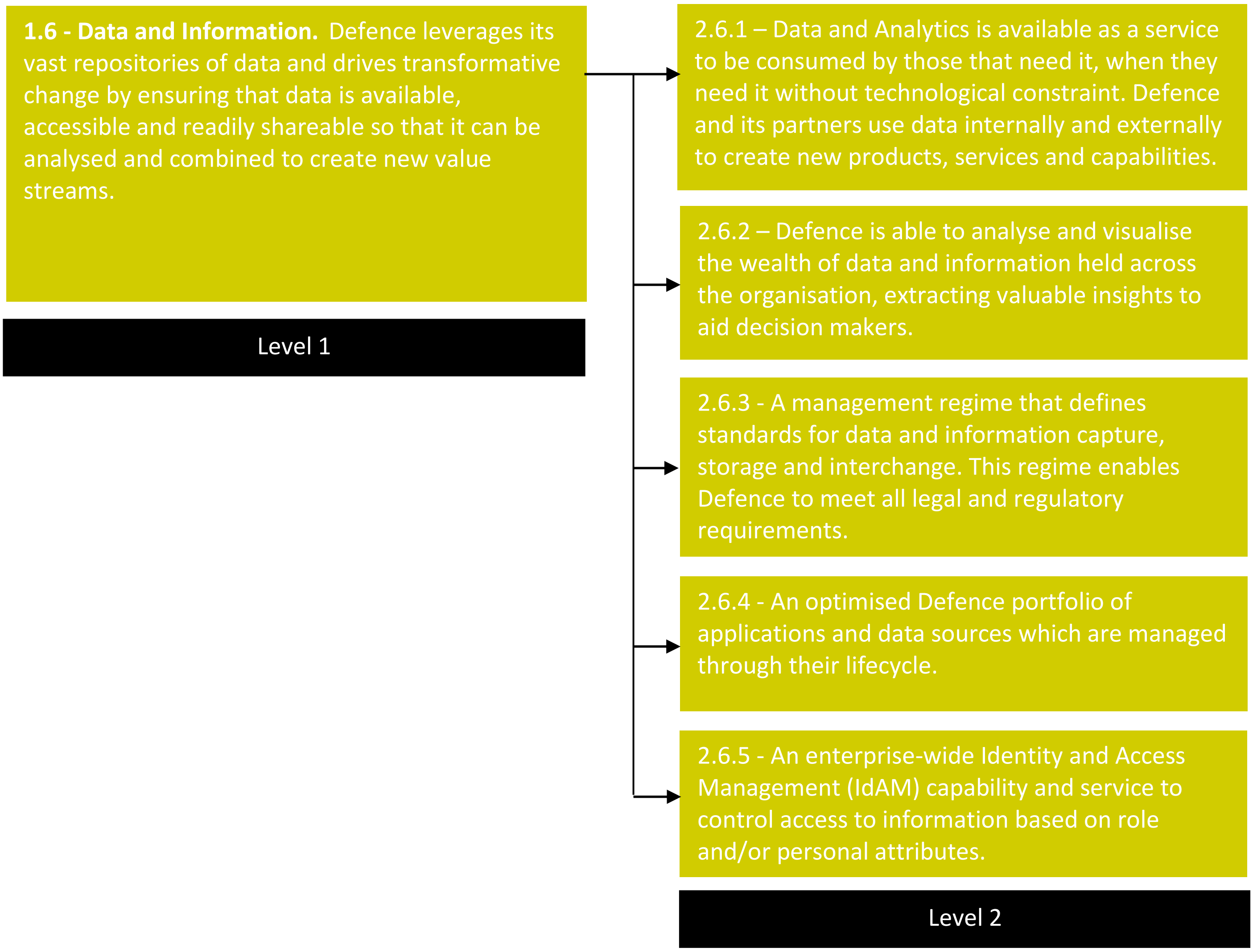
2.5.2 - Defence has an appropriately skilled information workforce to operate information capabilities.

2.5.3 - Defence has an optimally sized, resourced, skilled and energised workforce to design, develop and deliver current services and its portfolio of programmes and projects.

2.5.4 - Departmental information professionals exploit industry and government skills standards and frameworks and collaborate to improve ways of working and the quality of information and data across defence.

2.5.5 - A defence culture which embraces new digital technologies and ways of working, challenges received wisdom, and adopts a disruptive approach to delivering Defence capabilities.

Level 2



1.6 - Data and Information. Defence leverages its vast repositories of data and drives transformative change by ensuring that data is available, accessible and readily shareable so that it can be analysed and combined to create new value streams.

Level 1

2.6.1 – Data and Analytics is available as a service to be consumed by those that need it, when they need it without technological constraint. Defence and its partners use data internally and externally to create new products, services and capabilities.

2.6.2 – Defence is able to analyse and visualise the wealth of data and information held across the organisation, extracting valuable insights to aid decision makers.

2.6.3 - A management regime that defines standards for data and information capture, storage and interchange. This regime enables Defence to meet all legal and regulatory requirements.

2.6.4 - An optimised Defence portfolio of applications and data sources which are managed through their lifecycle.

2.6.5 - An enterprise-wide Identity and Access Management (IdAM) capability and service to control access to information based on role and/or personal attributes.

Level 2