The Trust Imperative

Why secure transformation is a leadership challenge, not a technology challenge

Authors

Andy Kiln
Richard Caddick



The world is how we shape it

sopra steria

Executive summary



Defence transformation isn't being held back by a shortage of technology. Despite increased investment and technical maturity, many organisations still struggle to turn innovation into trusted operational capability. The greatest barriers are increasingly organisational, cultural and behavioural: building trust, changing established ways of working and ensuring people are ready to adopt new capabilities. Technology provides the mechanism for change, but leadership, culture and adoption determine whether that change succeeds.

We had discussions with dozens of practitioners within the Aerospace, Defence and Security space working at the frontline of client delivery including transformation directors, CTOs, client directors, AI specialists and security leads. The practitioners work across some of the UK's most demanding environments, and a consistent message emerged: successful transformation depends less on technology choices and more on trust, collaboration, leadership and organisational behaviour.

The central point of this whitepaper is that trust is not simply an outcome of secure transformation. It's a prerequisite for it. In this paper, trust means justified confidence that people, organisations, data and systems will behave as expected, within clear and verifiable boundaries. Secure transformation succeeds when leaders create the conditions for that confidence: putting organisational change at the heart of technology adoption, making security a continuous partnership, establishing trusted foundations for agility and building ecosystems that can turn innovation into operational capability at speed.

Secure by Design is changing how organisations approach assurance. Zero Trust is reshaping assumptions about access and control. Sovereign cloud and AI are creating new opportunities, threats and challenges, while introducing new governance considerations. However, none of these initiatives succeed in isolation.

What connects these initiatives is trust: between organisations, suppliers and customers; in data and governance; and in the systems underpinning mission-critical operations.

The organisations that will succeed won't necessarily have the most advanced technology. They'll be the ones that can adopt it securely, confidently and at operational speed. They will be those capable of building trusted ecosystems that balance security, agility, innovation and resilience simultaneously.

This paper argues that secure transformation succeeds when leaders create the conditions for trust: treating organisational change as central to technology adoption, making security a continuous partnership, establishing trusted foundations for agility, and building ecosystems that can turn innovation into operational capability at speed.

Technology isn't the hardest part



The technology is often the easy part. The business change is much harder."

Marc Harry

Transformation Programme Director, Sopra Steria

Technology programmes rarely fail because the underlying technology doesn't work.

More often, they struggle because organisations underestimate the scale of behavioural, cultural and leadership change required to realise value from that technology. This observation was repeated throughout our discussions, regardless of whether the subject was cloud adoption, Secure by Design, AI or broader transformation initiatives.

Historically, many defence and government projects focused heavily on technical delivery. Security requirements were documented, systems were built, accreditation processes were completed and delivery milestones were achieved. Yet successful deployment did not always translate into successful adoption.

As Marc Harry observed, organisations can receive exactly the solution they requested and still fail to achieve the expected benefits if users are not prepared, leaders aren't aligned and operational change hasn't been properly managed. Business readiness cannot be treated as an afterthought. It must be considered a core component of transformation.

This challenges a common assumption in large programmes. Technology transformation is often treated as a technical exercise supported by organisational change. In reality, the reverse may be closer to the truth. Technology provides the mechanism for change, but leadership, culture and adoption determine whether the change succeeds.

That distinction is subtle but profound. It's why we put human-centred business change - grounded in people's needs, understanding and behaviours - at the heart of our transformation programmes.



Security must become a partnership



Security should no longer be viewed as a gate at the end of delivery."

Sue-Ellen Wright
Managing Director
Aerospace, Defence and Security
at Sopra Steria

One of the most significant developments in recent years has been the move from traditional accreditation models towards Secure by Design and continuous assurance approaches.

Continuous assurance, not one-time approval

For many organisations, the move from traditional accreditation to Secure by Design represents more than a procedural change; it requires a fundamental shift in mindset. Traditional accreditation often positioned security as a point in time assessment conducted late in the delivery lifecycle, where specialist teams reviewed a largely completed solution and decided whether the remaining risks were acceptable. Secure by Design replaces this approach with a model of continuous assurance, embedding security throughout the entire lifeycle from development and design through to delivery and operation. This shift moves responsibility for security to start earlier and monitor continuously, helping organisations identify and address risks proactively rather than retrospectively.



Keeping pace with the threat

Adversaries operate continuously, making periodic assurance insufficient. Maintaining a continuous understanding of vulnerabilities, threats and controls enables organisations to:

- identify and address risks earlier,
- adapt safeguards as threats evolve,
- make better-informed decisions throughout delivery, and
- strengthen security without creating a late-stage barrier to progress.

Secure by Design therefore shifts security from a final gate to an ongoing discipline, one that supports faster, safer and more resilient delivery.

Ethical hacking should therefore be embedded within delivery. By testing emerging designs from an attacker's perspective, security specialists can expose weaknesses early, help teams understand how an attack might unfold and enable improvements before vulnerabilities become costly to resolve.

In practice, this means security becomes a collaborative discipline rather than an adversarial one.

Several interviewees highlighted that successful outcomes increasingly depend on close partnership between customer organisations and industry. Solutions are rarely developed independently and presented for acceptance. More commonly, they emerge through continuous engagement, shared understanding and iterative decision-making.

Barry Weeks, Account Chief Technology Officer at Sopra Steria said "The process of security begins from the outset. It's not something you pass as a gate to the end, but it's a journey that you go on from beginning to end with every design decision you make and every step of the way."

The implications extend beyond security. When organisations embrace this approach, governance improves, decision-making accelerates, risk is understood earlier and trust grows between delivery teams and stakeholders. In short, Secure by Design is not only changing how security is delivered; it's changing how organisations work together.

Agility depends on trusted foundations



Mission teams can be agile because they operate on infrastructure that is already trusted."

Neil Salter

Director, National Security at Sopra Steria

One of the most persistent myths in secure environments is that security and agility are opposing forces. Our discussions pointed to a different conclusion: strong security foundations can increase agility. The most agile organisations are often those operating on the strongest security foundations.

Mission teams can respond rapidly because they trust the infrastructure, processes and governance that underpin their operations. They can experiment because clear boundaries exist. They can innovate because foundational risks have already been addressed.

This perspective reframes the so-called security paradox. Rather than asking how much security should be sacrificed to achieve agility, leaders should ask whether the right security foundations have been established to enable agility safely. This distinction matters because it influences investment decisions: when security is viewed purely as a constraint, spending can be perceived as overhead; when it's understood as an enabler, trusted infrastructure becomes a strategic asset.

This is particularly relevant as organisations explore AI adoption, data-sharing initiatives and multi-organisational collaboration models. These capabilities depend on confidence in underlying controls, governance and operating environments. Without trusted foundations, innovation inevitably slows because risks become harder to understand and manage.

Leaders shouldn't trade security for agility. They should invest in security that makes agility possible.



The future belongs to trusted ecosystems



Trust takes years to build and minutes to lose."

David Taylor

Client Director, Sopra Steria

Perhaps the most striking conclusion from our discussions is that trust may be becoming the defining leadership challenge of secure transformation.

Technology and capabilities can be acquired or developed, and processes can be implemented. Trust is different: it's earned through consistent, competent delivery and a demonstrated commitment to shared purpose. It develops over time and can be lost quickly.

In complex defence and government environments, trust performs a practical function: it allows organisations to collaborate across boundaries, helps leaders make decisions in conditions of uncertainty, enables innovation without introducing unacceptable risk, and creates confidence that suppliers, partners and customers are working towards shared outcomes.

This matters because transformation is becoming increasingly ecosystem-based. No organisation operates alone, and partners of different sizes and specialisms need meaningful opportunities to contribute their expertise and challenge assumptions. Cloud platforms involve multiple partners; AI capabilities depend on data providers, infrastructure providers and governance frameworks; and national resilience depends on collaboration between government, industry and allied organisations. Even sovereignty increasingly requires trusted collaboration rather than isolation.

As a result, the most important capability may not be technical expertise alone, but the ability to create and sustain trusted ecosystems. Several contributors reinforced this point by describing the importance of understanding customer context deeply, adapting to different operational environments and helping customers solve problems rather than simply delivering services. Although difficult to measure, these capabilities often determine long-term success.

For leaders, this creates a new challenge: success can no longer be evaluated solely through programme metrics, compliance measures or technical outcomes. Increasingly, leaders must also ask whether their partners trust them, whether their teams trust one another, whether users trust the systems they are asked to adopt, and whether governance processes enable or undermine that trust.

The answers to those questions may increasingly determine whether transformation succeeds.



Innovation requires trust

The technologies shaping Defence over the next decade will emerge from a diverse innovation landscape spanning government, industry, academia and specialist technology providers. Advances in AI, autonomous systems, secure collaboration and data exploitation will depend on combining the fresh thinking and agility of emerging providers with the scale, assurance and operational experience of established Defence partners.

Recognising the strategic importance of innovation, the UK Government, through the **£500m AI Investment Fund**, and MOD, through the **Defence Investment Plan**, are actively encouraging greater participation from SMEs and emerging technology and AI providers. These organisations often bring fresh thinking, specialist expertise and the agility to develop new capabilities rapidly. They play an increasingly important role in strengthening sovereign capability and accelerating the adoption of emerging technologies.

However, innovation alone does not create operational advantage. New ideas must be integrated into complex operational environments, aligned with security and governance requirements, and trusted by the people who depend on them. The challenge is not simply generating innovation. It's turning innovation into trusted capability. This requires collaboration between organisations that bring different strengths to the mission.



The future therefore belongs to trusted ecosystems: networks of organisations that combine innovation with assurance, agility with resilience and specialist expertise with proven delivery. Within these ecosystems, trust acts as the bridge between invention and adoption. It allows Defence customers to access the best emerging capabilities while maintaining confidence in security, sovereignty and mission assurance. In these ecosystems, established Defence partners play a critical role. Their value lies not only in the capabilities they develop themselves, but also in their ability to identify promising innovations, integrate them into complex programmes and help customers adopt them with confidence. By combining their own innovation with the creativity of specialist partners, they can accelerate the delivery of operational outcomes while reducing risk and increasing resilience.

Chief Scientific Advisers can play a pivotal role within these ecosystems. Positioned at the interface between scientific evidence, policy, operations and industry, they help leaders understand emerging technologies, challenge assumptions and judge where innovation can create genuine mission advantage. Their ability to provide independent scientific challenge and work across organisational boundaries allows them to act as trusted brokers: connecting specialist expertise with senior decision-makers, convening partners around shared problems and ensuring that scientific opportunity is balanced with security, ethics, operational need and evidence. In this way, Chief Scientific Advisers help reduce uncertainty and accelerate the journey from promising idea to trusted operational capability.

Trust determines how quickly Defence can turn innovation into operational advantage. This can be understood through the OODA loop: observing changing conditions, orienting to their significance, deciding how to respond and act. Originally developed by military strategist Colonel John Boyd, the OODA loop describes how individuals and organisations gain advantage by sensing, understanding and responding to events more quickly and effectively than their competitors or adversaries.

Trusted relationships, data, governance and decision-making reduce friction at each stage, enabling organisations to share insight, reach decisions and act faster than the threat while maintaining security, sovereignty and mission assurance.

Conclusion: trust as strategic advantage

The critical question for Defence leaders is not which technologies are available, but how quickly they can turn them into trusted operational advantage. Secure by Design, Zero Trust architectures, sovereign cloud platforms, artificial intelligence and emerging digital capabilities all offer significant opportunities to improve mission effectiveness, operational resilience and decision-making. Realising that value, however, depends on whether these capabilities can be adopted and exploited with the confidence of people, partners and stakeholders.

Throughout this paper, a consistent theme has emerged. The greatest barriers to secure transformation are rarely technical. They are organisational, cultural and behavioural. Success depends upon leadership teams creating environments where security enables rather than constrains, where risk is managed rather than avoided, and where collaboration can flourish without compromising mission assurance. Trust is the foundation that makes this possible.

This principle applies equally to the technologies shaping Defence's future. Secure by Design requires trust between delivery teams and security professionals. Zero Trust architectures depend on confidence in identity, governance and continuous assurance. Sovereign AI requires trust in data, models and decision-making processes. Digital sovereignty depends upon trust in technology choices, supply chains and strategic partners. In every case, trust is not the outcome of transformation. It's the prerequisite for it.

The future therefore belongs to organisations that can sustain trust across every critical relationship: between leaders and teams, security and delivery functions, organisations sharing information and capability, and the wider ecosystem of government, industry and innovation partners. Those that do so will be best placed to accelerate transformation, strengthen resilience and exploit emerging technologies at pace.

Trust is often described as a soft factor. In reality, it's a strategic asset: enabling collaboration without compromising security, innovation without increasing risk and transformation without losing control. In an increasingly connected and contested world, trust is a source of competitive advantage.

The future belongs to organisations that can connect with confidence, protect what matters and turn trusted transformation into mission advantage.



Andy Kiln
Chief Technology Officer



Richard Caddick
Consulting Director

The world is how we shape it

sopra steria