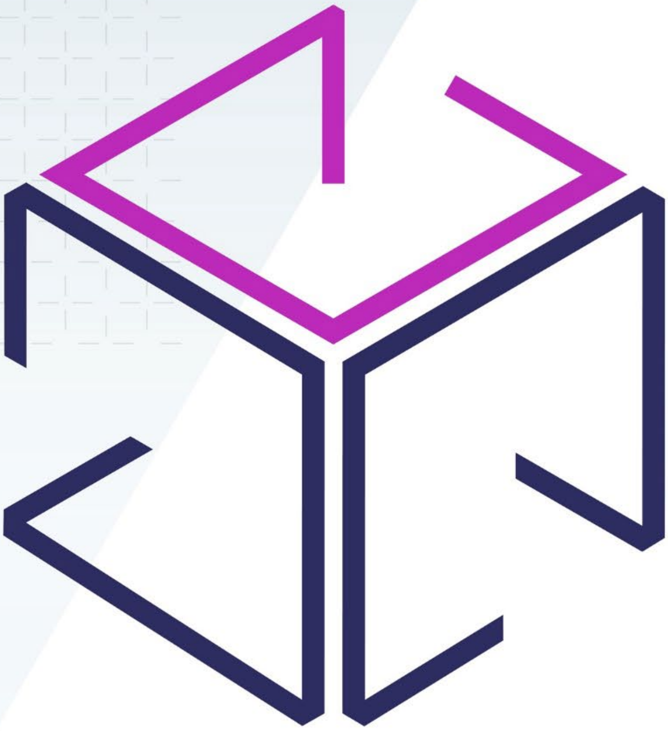
Workforce Foresighting Hub



Utilising Digital Twin Technology for Cybersecurity and Operational Modelling of Transport Tunnels

Workforce Foresighting Hub findings report in collaboration with the Connected Places Catapult.

Date: March 2025

UKRI Innovate UK

Right skills, right time, right place✓

Acknowledgements

The Workforce Foresighting process integrates data from the following international data sets:

IfATE – Institute for Apprenticeships and Technical Education, England

ESCO – European Skills, Competencies, Qualifications & Occupations, EU

ONet – Occupational Networks Online, USA

In accordance with licence and publishing requirements of these organisations for the use of their data sets, the Workforce Foresighting Hub team states that –

The IfATE data used contains public sector information licensed under the Open Government Licence v1.0.

The ESCO data is used in accordance with the EUROPEAN UNION PUBLIC LICENCE v. 1.2 EUPL © the European Union 2007, 2016

*The ONet data used is under CC BY 4.0 license. (O*NET® is a trademark of USDOL/ETA.) The Workforce Foresighting Hub team has modified all or some ONet information. USDOL/ETA has not approved, endorsed, or tested these modifications.*

Any errors, omissions and incorrect data are the responsibility of the Workforce Foresighting Hub team, and all queries should be addressed to info@iuk.wf-hub.org

The method and process used in the Workforce Foresighting process is under development and there may be errors and omissions in the data provided.

This report was produced following workshops undertaken November 2024 – February 2025 using the data set and tools available at that time.

Contents

Executive Summary

Executive Summary

This report outlines findings from the Workforce Foresighting cycle titled “Utilising Digital Twin Technology for Cybersecurity and Operational Modelling of Transport Tunnels”. The study is sponsored by National Highways and conducted by the Connected Places Catapult in collaboration with the Workforce Foresighting Hub, an Innovate UK initiative.

Workforce foresighting is a systemic approach to planning ahead and anticipating future skills and capability needs associated with new technologies and government transformation targets. It involves identifying and understanding the skills required for tomorrow’s jobs, ensuring our education and training systems are prepared so that our workforce is ready to adopt new technologies and support future industrial growth.

This report sets out the findings of the workforce foresighting study and suggests the next recommended actions required by educational institutions and employers to ensure the UK workforce is prepared to effectively implement these new technologies in the Sector.

Understanding the Challenge: National and Sectoral Perspective

Cybersecurity within UK transport infrastructure is facing an escalating challenge, coupled with historical gaps in securing legacy assets against malicious actors. As operational technology (OT) systems – such as ventilation controls, fire suppression, CCTV, power management, and others – become increasingly interrelated with information technology (IT) networks, they create new vulnerabilities and potential attack vectors. The convergence of these systems in transport tunnels introduces complex risks due to existing legacy infrastructure, constantly shifting cyber-physical threats, and the Sector’s limited cybersecurity expertise. Transport tunnels are particularly interesting for our challenge as they provide an environment rich with OT and IT, as these systems are deployed all around the tunnel surface and not only along or under the road surface.

The Cyber Security Skills in the UK Labour Market 2023 report highlights the severity of the issue, revealing that 50% of UK businesses lack basic cybersecurity skills and 33% are missing advanced capabilities. Additionally, 41% of organisations do not have the in-house expertise needed for incident response and recovery. Since 97% of organisations globally report IT incidents affecting OT and 46% have already suffered OT-specific breaches, the urgency to enhance workforce capabilities in transport cybersecurity is evident.

At the national level, the National Cyber Strategy 2022 and the Integrated Review Refresh 2023 both prioritise strengthening cyber resilience across the UK’s national critical infrastructure. These policies advocate for developing a highly skilled workforce capable of responding to cyber-physical threats in complex environments like tunnels. Our foresighting cycle aligns with these strategic goals by focusing on the intersection of digital twin technology (and, more specifically, “digital shadows”) and cybersecurity workforce readiness.

Technology Solutions Considered and Selection Rationale

To address these challenges, we considered and evaluated two technological interventions:

1. AI-driven automation for security and maintenance monitoring: leveraging machine learning to detect threats and assess infrastructure condition in real-time. This suite of technologies reduces reliance on manual monitoring, improving response times to cyber incidents and, potentially, shifting the focus from reactive to proactive threat mitigation.
2. Digital twins for system modelling, verification, and workforce training: digital twins enable simulation of cyber threats and operational failures in a sandbox (i.e., a safe environment for threat assessment and upskilling the workforce without fear of missteps on 'live' systems).

Following a structured evaluation, digital twins, specifically 'digital shadows', were selected as the primary solution for workforce foresighting in this cycle. Unlike real-time connected digital twins, which introduce cybersecurity vulnerabilities, our focus on digital shadows employs *static digital twins* that are built using historical data and predefined scenarios. This approach ensures a balance between enhanced predictive capabilities and cybersecurity risk mitigation. In this report, we will use the shorthand 'digital twin' to signify 'digital shadow'. Digital twins serve as a dual-purpose tool:

- Security Modelling – Used to simulate cyber-physical attack scenarios and evaluate defensive strategies in transport tunnels (i.e., Red Teaming).

- Workforce Development – Integrated into training frameworks to equip professionals with critical OT/IT cybersecurity skills, de-risking training as the workforce does not have to interact with 'live' technologies.

We decided not to focus on AI technologies because, although they show promising signs and are expected to have a significant impact on the Sector, their Technology Readiness Level and industry adoption are low. This factor alone eliminates these technologies from being the focus of the cycle, as the Workforce Foresighting programme specifically looks at technologies forecasted to coming to fruition on the UK market in Horizon 2 (i.e., 2-5 years from the time of writing this report).

Forecasted Industry Impact

This workforce foresighting cycle establishes the foundation for a more secure, skilled, and adaptive transport Sector, aligning with both UK government strategy and industry priorities. Still, we expect the adoption of digital twins within cyber-physical security strategies to require significant industry transformation:

- Workforce Demand Growth:
  - Increased need for cybersecurity specialists trained in OT/IT convergence. We expect cross-training to be an important factor
  - Expansion of roles focused on incident response, digital forensics, and predictive analytics and maintenance

- New Skills and Training Pathways:
  - Development of specialist cyber-physical risk analysis courses

    - Upskilling and cross-training existing professionals through simulation-based learning

- Economic and Security Benefits:
    - Reduction in operational downtime and potential security and financial losses from cyber incidents. We recognise that estimating the cost of downtime across the National Highways network is a complex exercise that, while being outside the scope of our research, still needs to be addressed
    - Improved national resilience against cyber threats targeting critical transport infrastructure

Participants and stakeholders

Employers	Educators	Technologists
Lead: Keith Price – National Highways	**Lead:** Abdullahi Arabo - University of the West of England	**Lead:** Tim Parker – PA Consulting
Oliver Lacey – National Highways	Navid Abapour – University of Surrey	Xicheng Li – University of Glasgow
Stephen Luke – National Highways		Minesh Vaghjiani – Department for Transport
Mark McAleer – BDO		Pavlos Padadopoulos – Edinburgh Napier University
Andrew MacLachlan – Cyber Warden		
Lizzy Morgan – Civil Aviation Authority		
Luke Martin-Farla – AtkinsRéalis		

The Findings and Insights

Our analysis of the foresighting cycle reveals an immediate imperative: bridging the workforce capability gap in cybersecurity within the transport infrastructure Sector – especially as digital twin technology becomes more integral to day-to-day operations in the Sector. As OT increasingly intertwines with IT, transport tunnels and other critical assets are exposed to a complex and shifting landscape of increasingly sophisticated and persistent cyber threats. Yet, our current workforce lacks the depth of expertise required to utilise digital twin-enabled security solutions, particularly in simulation engineering, cybersecurity risk modelling, and cyber-physical security simulation.

Introducing digital twins – which enable comprehensive cybersecurity testing, risk assessment, and immersive workforce training without jeopardising live infrastructure – represents a hard-to-miss opportunity. These virtual replicas serve as controlled, high-fidelity platforms for identifying vulnerabilities and simulating potential attack scenarios before threats can manifest in the real world. However, the full potential of these technologies can only be realised by the Sector through a coordinated effort to upskill professionals.

The widespread adoption of digital twin technology for cybersecurity and operational modelling is poised to fundamentally reshape and improve organisational strategies in managing cyber resilience across transport infrastructure. Key benefits include, but are not limited to:

- **Enhanced Cybersecurity Risk Modelling:** Digital twins facilitate scenario-based simulations of cyber-physical attack vectors. This proactive approach enables organisations to pinpoint vulnerabilities and develop precise, targeted defence strategies before malicious agents or coordinated offensive action strikes.

- **Improved Incident Response and Resilience Training:** Digital twins enable cybersecurity teams to test, validate, and refine response protocols without compromising live systems by providing a secure sandbox environment. This aspect sharpens operational readiness and accelerates the learning curve for new threats.

- **Bridging the OT/IT Skills Divide:** Effectively integrating OT and IT systems necessitates a workforce adept in both domains. Digital twin platforms create contextual, up-to-date and high-fidelity learning environments where professionals can acquire and hone the cross-functional skills essential for integrated cyber-physical security.

- **Integration of AI-Driven Security Monitoring:** Deploying digital twins is the first step towards coupling them with AI to accelerate anomaly detection and predictive maintenance. Automated security monitoring enhances response times and reduces the operational burden on human teams, freeing up resources for strategic tasks.

- **Alignment with Regulatory and Compliance Frameworks:** As regulatory bodies demand increasingly rigorous cyber-physical security assessments, digital twin-based validations offer a transparent approach. This ensures that risk assessments comply with existing standards and evolve to meet emerging regulatory demands.

Adopting digital twin technology promises to shift the transport Sector's cybersecurity model from reactive, *post hoc* (metaphorical) firefighting to a predictive, intelligence-driven, and adaptive paradigm. This proactive stance we advocate for is necessary for safeguarding critical national infrastructure, maintaining public trust, and ensuring the long-term resilience of our national transport networks.

Future-Oriented Pathways (FOPs) Identified

This foresighting cycle has identified a range of new and evolving workforce roles that will be essential for deploying and maintaining digital twin security solutions in transport infrastructure. These Future-Oriented Pathways (FOPs) are:

- **Senior-Level Roles**
  - Senior Research Scientist (Simulation) – Leading the development of digital twin-based security simulations
  - Senior Cybersecurity Innovation Lead – Driving the strategic integration of digital twin technology into cybersecurity operations
  - Senior Compliance Officer (Simulation) – Ensuring regulatory alignment of digital twin-based security practices
  - Senior Cybersecurity Auditor – Evaluating digital twin applications for compliance with cybersecurity standards

  - Senior Digital Twin Specialist – Overseeing the deployment and iterative refinement of digital twin models for security testing

- **Mid-Level Roles**
  - Prototyping Engineer – Developing proof-of-concept digital twin security models
  - Software Developer – Creating simulation environments for cyber-physical security testing
  - Cybersecurity Specialist – Managing digital twin-enabled threat modelling and response strategies
  - BIM Specialist – Integrating Building Information Modelling (BIM) with digital twin security solutions
  - Systems Integration Specialist – Ensuring the integration of digital twins within OT/IT security frameworks
  - Cybersecurity Consultant – Advising on best practices for digital twin-enabled cybersecurity
  - Compliance Officer – Aligning digital twin applications with regulatory security requirements
  - Digital Twin Specialist – Managing digital twin models for security simulations and predictive maintenance
  - Simulation Engineer – Designing and testing cyber-physical threat scenarios within digital twin environments
  - Project Manager – Overseeing the implementation of digital twin cybersecurity initiatives
  - Software Test Engineer – Validating digital twin applications for cybersecurity resilience

- **Junior-Level Roles**
  - Digital Twin Engineer – Assisting in the deployment and maintenance of digital twin security solutions
  - Data Analyst – Analysing threat data generated by digital twin simulations to identify vulnerabilities

Workforce Capability Strengths and Gaps

This foresighting cycle confirms that the UK's workforce possesses significant strengths when it comes to cybersecurity – a solid foundation that can be enhanced with digital twin expertise. The nation already boasts a well-established cybersecurity workforce with proficiency in incident response and risk assessment. Moreover, experts in Machine Learning within the are well-positioned to develop predictive analytics models that can underpin digital twin platforms. Further, software developers and systems integration experts bring a wealth of relevant experience that can be readily applied to digital twin security modelling. These strengths illustrate a robust baseline of technical capability and innovation potential that could serve as a springboard for further advancements in cybersecurity through digital twins.

In contrast, critical gaps must be addressed to fully introduce and deploy digital twin technology for securing transport infrastructure. Despite the strong overall cybersecurity foundation, this cycle highlights a notable shortage of professionals trained explicitly in digital twin applications for cybersecurity, which hampers developing, deploying, managing and maintaining secure digital twins. Additionally, many cybersecurity experts currently lack the specialised experience required for managing the convergence of OT and IT. Finally, there is limited expertise and explicit policy guidance in navigating the regulatory frameworks necessary to ensure compliance with national cybersecurity.

While the existing strengths provide a promising platform for innovation, the stark contrasts with the identified workforce gaps emphasise the urgent need for comprehensive upskilling and strategic training interventions.

The Next Steps

The findings of this foresighting cycle spotlight an urgent need for targeted workforce interventions to support the integration of digital twin technology in cybersecurity for transport infrastructure. We propose a series of strategic interventions to move this agenda forward.

First, a cross-sector working group should be established, bringing together representatives from industry, academia, the Institute for Apprenticeships and Technical Education (IfATE), and Innovate UK while actively engaging organisations such as National Highways and Connected Places Catapult to ensure alignment with industry needs. The Future Occupational Profiles (FOPs) introduced above should be validated and refined through further engagement with training providers, professional bodies, and employers so that the curriculum reflects real-world demand and emerging cyber threats.

This report also calls for the development of a detailed action plan that sets short-term upskilling measures, pilot training programmes, and mid-term objectives to incorporate digital twin-based security training into formal qualifications and apprenticeships, ensuring alignment with national cybersecurity policies. Finally, opportunities for additional foresighting studies will be evaluated to explore the potential of digital twins in enhancing cyber-physical security beyond road transport, including the maritime and aviation Sectors, as well as other forms of transport, and non-transport Sectors.

Failing to implement these measures would leave the UK’s transport Sector dangerously exposed to a growing array of cyber threats. Without decisive action to develop a highly skilled workforce capable of implementing digital twin-enabled cybersecurity solutions, the current skills gap will widen, leaving critical transport infrastructure increasingly vulnerable.

Such inaction will result in heightened financial and operational risks as delays in adopting proactive security measures allow threats to materialise. Moreover, the inability to develop and maintain a future-ready workforce would undermine the competitiveness of the UK’s transport and cybersecurity Sectors in the global economy. Thus, while the steps outlined above offer a pathway to transform workforce capabilities and safeguard our national infrastructure, the cost of inaction is measured not only in escalating risks and economic losses but also in the potential forfeiture of the UK’s leadership in cybersecurity on the global stage.

1. Introduction

1. Introduction

1.1 Background to Workforce Foresighting

The report "Manufacturing the Future Workforce" (Collier et al., 2020) recommended the Skills Value Chain as an approach to avoid shortfalls in workforce capabilities relating to future innovations (see Figure 1). This is the genesis of the workforce foresighting programme, which is sponsored by Innovate UK and delivered through the Innovate UK Catapult Network.

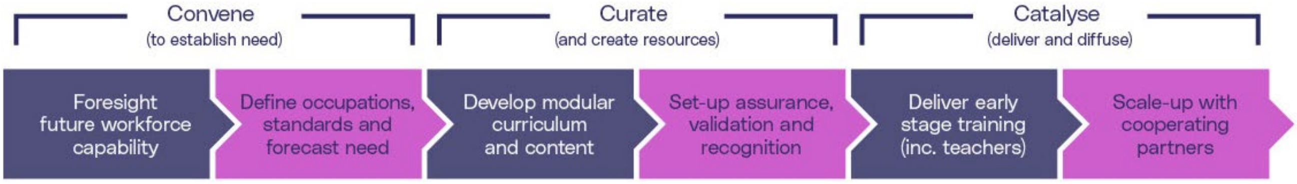

Convene
(to establish need)
Curate
(and create resources)
Catalyse
(deliver and diffuse)
Foresight future workforce capability
Define occupations, standards and forecast need
Develop modular curriculum and content
Set-up assurance, validation and recognition
Deliver early stage training (inc. teachers)
Scale-up with cooperating partners

Figure 1: The Skills Value Chain

The first step of the skills value chain is to "Foresight future workforce capability": This calls for technology, industry, education, and training partners to convene using government as a focal point, to "foresight and articulate future skills needs, standards and qualifications associated with emerging technologies" (Collier et al., 2020).

1.2 Workforce Foresighting - Process Overview

The core of workforce foresighting is convening three groups of relevant specialists to conduct structured, Delphi-style, facilitated workshops to capture and discuss the set of organisational capabilities that will be required to respond to and exploit technology innovation.

Organisational capabilities are captured using a bespoke classification that has been developed by the Workforce Foresighting Hub. The classification uses a structured common language to enable cross-sector and cross-centre collaboration and integration of data. Additionally, the classification enables data from a number of other national and international open-source workforce datasets to be integrated through the same common language. The data is held in a cloud based "data-cube" that is dynamically growing as each workforce foresighting cycle adds to the shared data relating to future workforce capabilities.

Using cutting edge AI and Large Language Model data tools, the data-cube is used to undertake detailed analysis to 'map' future workforce capability requirements against the current education and training provision to identify where existing provision can be used and where new provision, CPD or qualifications are required.

As an agile development project, the Workforce Foresighting Hub team are constantly evolving and improving the detailed workshop process and workshop approach, but always consists of the following stages:

Considering – Clarifying the Challenge to be met (the 'what' and the 'when') and collating solutions (the 'how') as foresighting topic suggestions align with strategic priorities

Identifying – Gain clarity and consensus about the solutions to be put forward – make the case for foresighting

Preparing – The convening of specialists and scheduling of workshops

Carrying out – Run foresighting workshops with experts, collate and analyse data

Communicating – Insights, findings and recommendations gathered from all research in report

Causing action – The driving of action based on the recommendations (promoting progress down the rest of the skills value chain) built on the findings and recommendations of foresighting

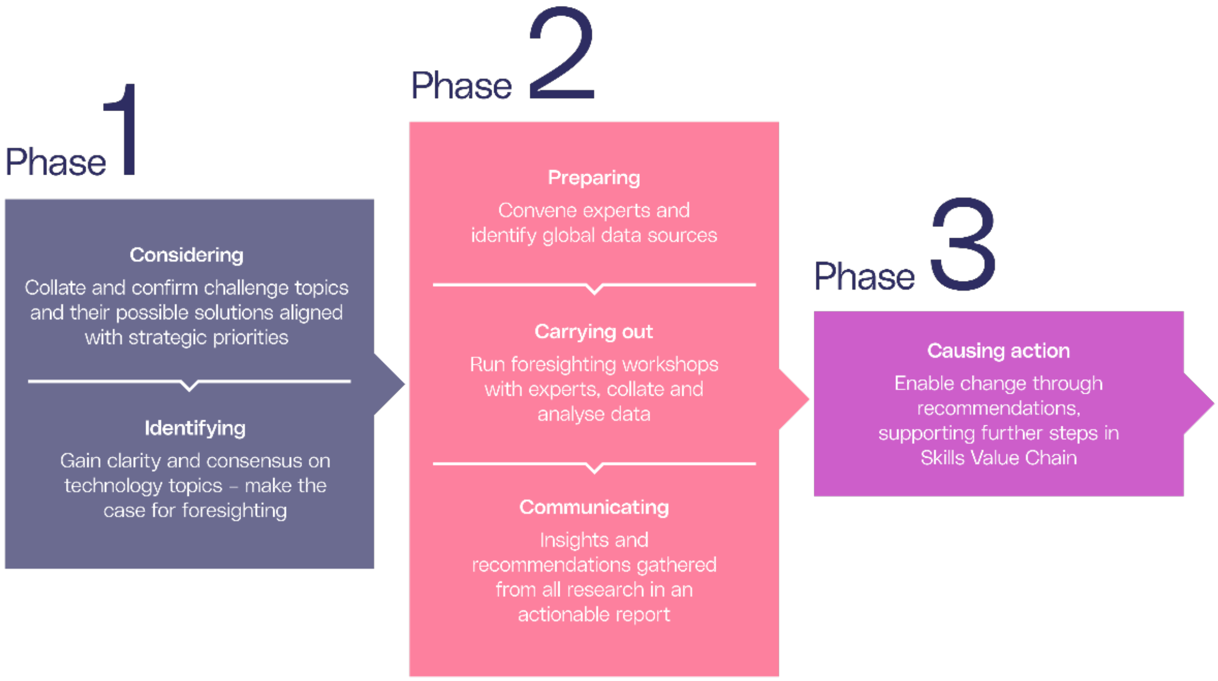

Phase 1
Considering
Collate and confirm challenge topics and their possible solutions aligned with strategic priorities
Identifying
Gain clarity and consensus on technology topics – make the case for foresighting
Phase 2
Preparing
Convene experts and identify global data sources
Carrying out
Run foresighting workshops with experts, collate and analyse data
Communicating
Insights and recommendations gathered from all research in an actionable report
Phase 3
Causing action
Enable change through recommendations, supporting further steps in Skills Value Chain

Figure 2 - The workforce foresighting process

1.3 Foresighting vs Forecasting

Although this study is focussed on workforce foresighting (capabilities required) it is important to keep in mind parallel findings from forecasting (required capacities and numbers). Forecasting, alongside foresighting, provides vital input to the Sector, feeding into recruitment and development targets for employers, and consideration of economic class sizes and recruitment targets for educators. However, it is beyond the scope of the foresighting study to carry out independent forecasting, and as such readers should refer to referenced studies for detail on forecasting.

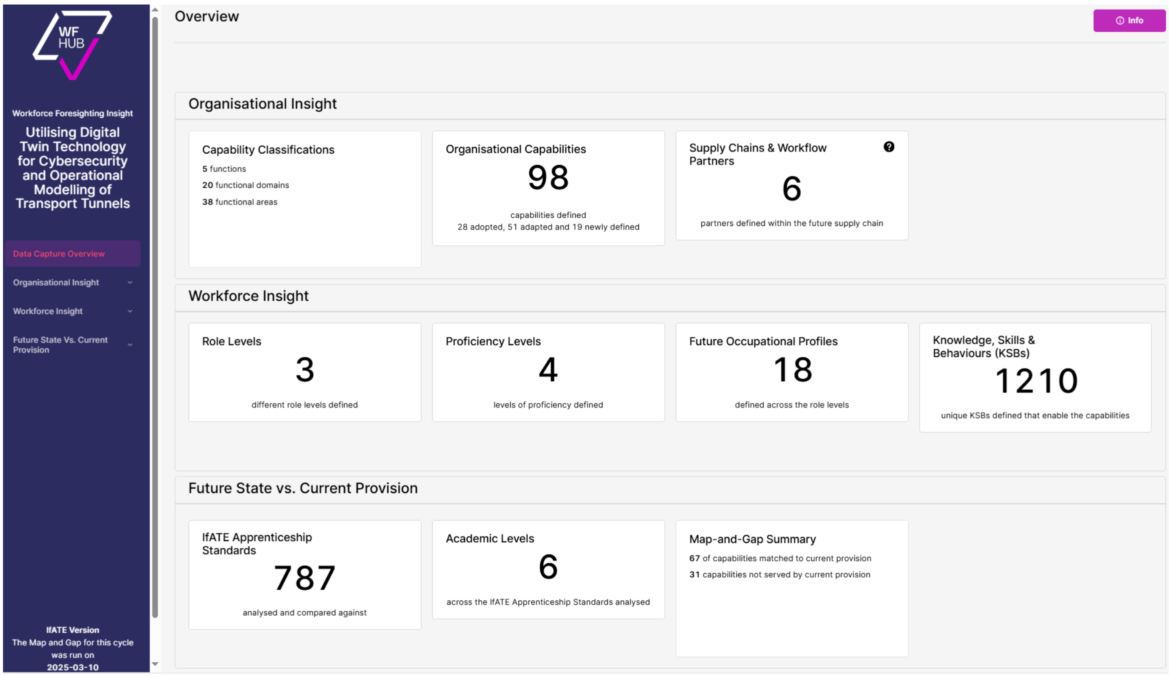
1.4 Introducing the Visualisation Tool

The Workforce Foresighting Hub's Visualisation Tool is a powerful, innovative system, which will enable the reader to explore and analyse foresighting data to determine the capabilities required for future roles. Links throughout this report make it easy to identify existing standards which meet the needs of these future roles and pinpoint where new standards are necessary to develop a skilled workforce equipped to adopt new technologies.

The data is generated by the foresighting cycles, integrating the expertise of technologists/ domain specialists, employers and educators. The data informs the development of future curriculums and course content as determined by the action plan. Using AI tools validated by human oversight, and by linking to external data sources, the tool identifies differences at the level of occupation/role as well as detailed changes required to help update/refresh knowledge, skills and behaviours thus delivering insights for learners, providers, creators and assurers of skills.

Detailed instructions on how to use the Visualisation Tool can be found in the appendix.

Link to Visualisation Tool



Workforce Foresighting Insight

Utilising Digital Twin Technology for Cybersecurity and Operational Modelling of Transport Tunnels

IfATE Version
The Map and Gap for this cycle was run on
2025-03-10

Overview

Organisational Insight

Capability Classifications
5 functions
20 functional domains
38 functional areas

Organisational Capabilities
98
capabilities defined
28 adopted, 51 adapted and 19 newly defined

Supply Chains & Workflow Partners
6
partners defined within the future supply chain

Workforce Insight

Role Levels
3
different role levels defined

Proficiency Levels
4
levels of proficiency defined

Future Occupational Profiles
18
defined across the role levels

Knowledge, Skills & Behaviours (KSBs)
1210
unique KSBs defined that enable the capabilities

Future State vs. Current Provision

IfATE Apprenticeship Standards
787
analysed and compared against

Academic Levels
6
across the IfATE Apprenticeship Standards analysed

Map-and-Gap Summary
67 of capabilities matched to current provision
31 capabilities not served by current provision

2. Aligning the Challenge and Solutions with National Priorities

2. Aligning the Challenge and Solution with National Priorities

2.1 Positioning and Context of National Challenge

The UK government has strategically positioned cybersecurity resilience as a cornerstone of its national infrastructure agenda, recognising that the convergence of Operational Technology (OT) and Information Technology (IT) presents a formidable security risk. Flagship initiatives such as the National Cyber Strategy 2022 and the Integrated Review Refresh 2023 articulate a bold vision for the country to become a global leader in cybersecurity, particularly in protecting critical national infrastructure. However, the UK Cyber Security Skills in the Labour Market 2023 report paints a more challenging picture, reporting that half (50%) of UK businesses lack basic cybersecurity skills, while a significant proportion (33%) struggle with more advanced competencies such as breach analysis and threat intelligence. Moreover, nearly half of organisations (41%) report a lack of internal expertise for managing cyber incidents. This shortfall is detrimental to the security of complex cyber-physical environments with national security implications, like transport tunnels.

The stakes are exceptionally high within transport – a sector contributing over £60 billion annually to the UK's economy and supporting more than 1.6 million domestic jobs. As the industry embraces digital transformation through automation, analytics and data-driven decision-making, integrating legacy OT systems with modern digital technologies has introduced new vulnerabilities. Transport tunnels, exceptionally dense OT/IT environments, are now at heightened risk.

Internationally, most organisations (97%) have reported IT security incidents impacting OT systems, and almost half (46%) have experienced breaches specifically targeting these environments. Should the UK fail to develop the necessary cybersecurity skills, the nation risks lagging global competitors – especially in Europe and North America, where investments in bleeding-edge security solutions such as digital twin technologies are rising[1]. From a purely economic perspective, the global market digital twin technology is exceptionally promising and expected to grow at 37.5% Compound Annual Growth Rate (CAGR) between 2024 and 2030.

Looking to the future, technology evolution promises significant advancements in mitigating (and creating new) cyber risks within transport infrastructure. In particular, digital shadows mark a notable departure from their connected counterparts. While connected digital twins introduce live cyber risks by continuously interacting with operational systems, digital shadows offer a controlled environment ideal for testing, simulation, and workforce training. This controlled setting supports threat detection and cyber-physical sandboxing, enabling training the workforce on rapid response to emerging threats.

Further, as transport operators shift towards data-driven infrastructure security strategies, there will be a growing demand for a new class of professionals skilled in simulation engineering, cybersecurity, and IT/OT integration. Adopting these technologies is set to reshape the cybersecurity landscape, provided that immediate and focused workforce

[1] E.g., the European Union Digital Programme Europe (DIGITAL) has invested €108 million on the matter, with €55 million allocated specifically in specialised educational programmes in advanced digital skills.

interventions are implemented. In doing so, the UK can secure its position as a leader in cyber-physical resilience while ensuring that its transport networks remain robust against future cyber threats.

This foresighting cycle aligns with the priorities set out in key government reports and industry studies, including:

- National Cyber Strategy (Cabinet Office, 2022) – Emphasises the importance of securing critical national infrastructure through advanced cybersecurity capabilities and workforce development
- Integrated Review Refresh 2023: Responding to a more contested and volatile world (Cabinet Office, 2023) – Recognises the growing cyber threat landscape and the need for more significant investment in cyber resilience for transport infrastructure
- UK Cyber Security Skills in the Labour Market (Department for Science, Innovation and Technology & Viscount Camrose, 2023) – Highlights severe workforce shortages in cybersecurity, particularly in incident response, digital forensics, and OT security
- Forging the Human–Machine Alliance (McKinsey Digital, 2020) – Identifies human-machine collaboration as the future of cybersecurity, where AI enhances human decision-making rather than replacing it

The UK transport sector faces an urgent cybersecurity challenge as cyber-physical threats evolve, and digitalisation accelerates. Integrating digital twin technology into cybersecurity strategies offers an opportunity to enhance workforce capabilities, mitigate risks, and improve resilience. However, without strategic workforce development initiatives, the Sector will struggle to adapt, increasing the likelihood of security breaches and infrastructure disruptions. A coordinated approach involving government, industry, and training providers is essential to ensure the right skills are in place at the right time, positioning the UK as a global leader in cyber-physical security for transport infrastructure – and beyond.

To this effect, the challenge we focused on this Cycle was:

> *The UK's cybersecurity landscape is evolving rapidly, creating an increasing need for skilled workers. The "Cyber Security Skills in the UK Labour Market 2023" report reveals that 50% of UK businesses lack basic cybersecurity skills, and 33% lack advanced skills. This gap, combined with the rising complexity of cyber-physical systems in transport makes advanced cybersecurity measures essential. Using tunnels as an example, operational technology (OT) systems managing ventilation, fire suppression, CCTV, and power supply converge with information technology (IT), the risks of attack also converge. Legacy vulnerabilities, evolving threats, and infrastructure digitisation further exacerbate these risks. Integrating human-machine teams to enhance cybersecurity in such environments is a key approach, allowing the strengths of human intuition and machine precision to protect systems effectively.*

2.2 Potential and Prioritised Technology Solutions to the Challenge

We employed a structured evaluation process to identify the most viable technology solutions supporting cybersecurity resilience in transport tunnels. In this process, we rigorously assessed several technologies against criteria such as its relevance to mitigating cyber risks in OT/IT-integrated environments, its potential to create workforce skills gaps weighted against the benefits in enhancing cyber-physical security, its technical maturity and readiness for widespread deployment, the ease with which it could be integrated into existing transport security frameworks, and the projected timeline for its implementation. These criteria provided a grounding framework for comparing and contrasting potential solutions, ensuring we considered only those aligned with national cybersecurity priorities, workforce capabilities and the Horizon 2 (i.e., 2-5 years) timeline[2].

Among the various options evaluated, two key solutions emerged as particularly promising: (i) AI-driven security and (ii) digital twin technology. First, we recognised AI-driven security and maintenance monitoring automation as a powerful tool, harnessing machine learning and predictive analytics to enhance threat detection, reduce reliance on manual oversight, and enable proactive maintenance measures. These technologies can potentially speed up threat identification and response times significantly. However, AI-driven security's full potential is somewhat constrained by the current limitations in workforce expertise on the subject within the transport sector and its Technology Readiness Level.

Second, we highlighted digital twin technology for its capacity to create virtual replicas of tunnel infrastructure, allowing for safe simulation of cyber-attack scenarios, comprehensive cyber risk assessments, and immersive training environments. Although digital twin applications in cybersecurity are still emerging – particularly compared to their established role in structural integrity monitoring – they present an immediate and scalable solution for enhancing cyber-physical security in tunnels. The following Table summarises our considerations.

[2] The Three Horizons framework was developed by Sharpe et al. (2016) as follows. Horizon 1 (1-3 years): maintaining and defending the core business. Horizon 2 (2-5 years): nurturing emerging businesses and capabilities. Horizon 3 (5-10 years): creating genuinely new businesses.

Technology Option	Brief Description	Relevance to Challenge	Current State and Supply Chain Impact	Timing Considerations
AI-driven automation for security and maintenance monitoring	Uses machine learning and AI to automate security assessments, detect threats, and predict maintenance failures in transport tunnels.	Reduces reliance on manual monitoring, improves threat detection speed, and enables predictive maintenance to enhance cybersecurity resilience.	AI adoption in transport security is growing, but workforce expertise in AI-driven cybersecurity is limited. Supply chain includes AI developers, transport operators, and cybersecurity firms.	2026-2030 – AI models require training on transport-specific datasets before full implementation.
Digital twin technology for cybersecurity simulation and workforce training	Provides virtual models of tunnel infrastructure for security testing, cyber risk assessment, and training.	Supports cyber-physical security training, enables safe simulation of cyber-attack scenarios, and improves incident response strategies.	Digital twin adoption in cybersecurity is limited, with most applications currently focused on structural integrity monitoring rather than security. Supply chain includes software developers, cybersecurity firms, transport operators, and training providers.	2027-2032 – Digital twins can be developed using existing infrastructure data, but workforce upskilling is required for full adoption.

In comparing these two options, the AI-driven automation solution presents a clear advantage in streamlining operational monitoring and predicting maintenance failures. Yet, it is dampened by a relatively underdeveloped ecosystem of skilled practitioners. In contrast, while emerging, digital twin technology provides a safe platform for testing and training. It serves as a bridge to overcome longstanding challenges in integrating legacy OT systems with modern digital security measures. This point makes digital twins particularly effective in enhancing workforce competency through interactive, simulation-based training while simultaneously improving overall cybersecurity planning. Consequently, despite the merits of both solutions, the evaluation process ultimately prioritised digital twin technology as the most immediate and scalable approach to addressing the cybersecurity and skills challenges in the UK's transport infrastructure within the 2–5-year Horizon.

We recognise that the current state of digital twin adoption in the transport sector is characterised by a strong focus on structural monitoring and operational optimisation rather than cybersecurity applications. In major infrastructure projects, digital twins are already employed effectively for asset management and performance enhancement; however, their potential for securing transport tunnels against cyber threats remains largely untapped. This gap highlights a clear divergence between established practices and emerging cybersecurity needs. The industry has built a solid foundation in using digital twins to maintain and optimise physical assets. Yet, there is an urgent need to expand these applications to encompass robust cyber-physical risk modelling and threat simulation.

Supply chain considerations further complicate this matter. Software developers and cybersecurity firms must now broaden their focus to integrate nuanced cybersecurity threat models into existing digital twin platforms. Further, training providers and academic institutions are called upon to develop specialised courses that build the requisite skills in Security using digital twin. Transport operators and infrastructure managers, for their part, are expected to invest in digital twin-based risk analysis to enhance resilience against cyber threats. This approach inevitably requires collaboration among government agencies, industry regulators, cybersecurity specialists, and transport infrastructure providers.

The implementation timeline we identified in this research is structured into distinct phases that allow for a gradual and systematic transition. In the initial phase, envisioned between 2027–2028, the focus will be on designing and developing digital twin models tailored explicitly for cybersecurity simulation, alongside creating preliminary workforce training frameworks. This phase sets the groundwork by aligning technological capabilities with training needs. The next phase, spanning 2028–2029, involves pilot implementations where selected transport tunnels would deploy these digital twins to support incident response training and risk assessment. Finally, the integration phase, projected for 2029–2032, aims to roll out digital twin-enabled cybersecurity strategies across the national transport infrastructure, ensuring that these advanced solutions are fully embedded within the operational fabric of the Sector.

2.3 Workforce Foresighting for Chosen Prioritised Technology Solutions

The prioritised technology solution identified in this workforce foresighting cycle is digital twin technology for cybersecurity simulation and workforce training. Unlike traditional cybersecurity methods, which often rely on reactive measures and live testing environments that can inadvertently expose critical infrastructure to risk, digital twins offer a controlled, risk-free setting for modelling cyber-attack scenarios. This approach enables the simulation of cyber-physical threats in transport tunnels without endangering live systems, but it also provides an immersive training platform for security professionals, thereby addressing existing skills gaps in OT/IT security. Moreover, digital twins facilitate predictive security analytics, allowing transport operators to proactively identify and remediate vulnerabilities before they can be exploited, in contrast to conventional methods that may only detect issues *after* they occur.

This foresighting cycle positions digital twin technology as a strategy for enhancing national infrastructure resilience. The initiative is set within a Horizon 2 timeframe (2027–2032), with workforce upskilling beginning in 2027 to ensure the sector is prepared for emerging challenges.

The anticipated impact is significant: by integrating digital twin cybersecurity simulation into operational frameworks, workforce upskilling for threat detection and incident response will be markedly improved, thereby reducing the risk of cyber-physical disruptions. The scale of this transformation extends beyond transport tunnels, with implications for smart transport systems, energy infrastructure, and automated logistics networks. Successful deployment depends on a collaborative supply chain that spans research and development organisations, software developers, systems integration specialists, transport operators, the National Cyber Security Centre, and regulatory bodies. These stakeholders must work in unison to embed digital twin-enabled security solutions within the transport sector's operational framework, laying the foundation for long-term cybersecurity workforce resilience and ensuring that the UK can protect its critical infrastructure. The following Table summarises this cycle's scope and supply chain.

Factor	Description
Horizon	Horizon 2 (2027-2032) – The foresighting cycle targets a 5-year implementation period, with workforce skills development beginning in 2027 to ensure sector readiness.
Impact	The adoption of digital twin cybersecurity simulation will enhance threat detection, incident response, and security training, significantly reducing the risk of cyber-physical disruptions in transport infrastructure.
Scale	This workforce transformation will affect critical national infrastructure (CNI), with a focus on transport tunnels but with wider applications across smart transport systems, energy infrastructure, and automated logistics networks.
Supply Chain	Successful implementation requires collaboration across multiple sectors, each contributing essential expertise: • **Research and Development Organisations / Higher Education Institutions (HEIs):** Provide valuable insights into emerging trends in digital twin technology and cybersecurity. • **Software Development Companies / Suppliers:** Develop the software infrastructure necessary for the effective implementation of digital twin technologies. • **Systems Integration Specialists & Consultants:** Ensure seamless interoperability between operational technology (OT) and information technology (IT), enhancing overall efficiency and security. • **Transport Operators:** Offer insights into operational challenges and requirements while benefiting from improved cybersecurity and operational modelling. • **National Cyber Security Centre (NCSC):** Establishes standards and best practices to help organisations safeguard their digital infrastructure against cyber threats. • **Regulators and Auditors:** Ensure compliance with safety and operational protocols while assessing the effectiveness of cybersecurity measures in transport systems.

2.4 Current and Predicted Scale of Technology Deployment in UK

The impact of deploying digital twin cybersecurity solutions extends throughout the entire supply chain, necessitating a broad evolution among industry stakeholders. Research and development organisations and higher education institutions are vital in researching what is possible, pushing the limits of science and existing technology, without the need to be commercially viable. In contrast, software development companies and suppliers are essential for building the sophisticated digital platforms required for implementation of technologies that are not only feasible, but also viable. Systems integration specialists and consultants ensure that the various components (such as OT and IT) interconnect with little friction. Simultaneously, transport operators and infrastructure managers must adopt these new technologies, such as Digital Twins, to address operational challenges while the National Cyber Security Centre provides guidance and establishes best practices. Regulators and auditors further support the initiative by ensuring safety and operational compliance. In this way, each stakeholder group contributes uniquely to the successful deployment of digital twin cybersecurity, yet their coordinated efforts are indispensable for overcoming the prevailing challenges. The following Table summarises the supply chain stakeholders we considered during this Cycle.

Supply Chain Stakeholder	Role in Deployment	Impact
Research and Development Organisations / HEIs	These institutions focus on advancing knowledge through research and innovation. They collaborate with industry partners to develop new technologies and methodologies.	Provide valuable insights into emerging trends in digital twin technology and cybersecurity. Conduct experimental research pushing the limits of technologies, without the need for commercial viability.
Software Development Companies / Suppliers	These firms specialise in creating bespoke software solutions, including applications for cybersecurity and operational modelling.	Essential for developing the software infrastructure needed to implement digital twin technologies effectively.
Systems Integration Specialists & Consultants	These professionals assist organisations in integrating various technological systems and processes.	Ensure that different components, such as operational technology (OT) and information technology (IT), work together seamlessly, enhancing overall efficiency and security.
Transport Operators	These organisations manage and operate the transportation networks across the UK.	Provide insights into operational challenges and requirements, benefiting from improved cybersecurity and operational modelling.
National Cyber Security Centre	This government agency offers guidance and support on cybersecurity matters.	Crucial in establishing standards and best practices, helping organisations safeguard their digital infrastructure against cyber threats.
Regulators and Auditors	These bodies oversee compliance with regulations and standards in the transport sector.	Ensure that safety and operational protocols are adhered to and assess the effectiveness of cybersecurity measures implemented in transport systems.

2.5 Key Stakeholders

Stakeholder Category	Organisations Involved	Role in Deployment
Employer Participants	National Highways BDO Department for Transport Civil Aviation Authority	Lead implementation of digital twin security models, provide industry insights, and shape workforce training needs.
Educator Participants	University of the West of England University of Surrey University of Glasgow Edinburgh Napier University	Develop specialist training and research in cyber-physical security, digital twins, and OT/IT integration.
Technologist Participants	Cyber Warden AtkinsRéalis PA Consulting	Contribute to cybersecurity technology advancements, including AI-driven security analytics and digital twin threat modelling.

Successful implementation of digital twin cybersecurity solutions hinges on close collaboration among stakeholders across education levels and the larger supply chain. Specialist training programmes must be developed to equip cybersecurity professionals, engineers, and transport operators with the advanced skills needed to navigate this complex domain. Further, there is a critical need to establish and disseminate best practices for digital twin security modelling within transport tunnels, ensuring that robust, operationally sound and proven methodologies underpin technological innovations.

Moreover, aligning industry requirements with government cybersecurity policies and regulatory frameworks is essential to create a cohesive and resilient ecosystem. This alignment ensures that appropriate governance and compliance measures match technological advancements and bridge emerging industry capabilities and public policy.

3. Findings and Results

3. Findings and Results

3.1 Methodology and Findings

We provide here summary information with a narrative based on the underlying data which is also provided using bespoke visualisations to enable greater insight and access to detail. The report is aligned to the needs of those responsible for workforce planning – employers, educators, and other skills providers.

Step One – How will the Supply chain change - Organisational Changes

An exploration of changes to organisational capabilities provides insights into how organisations will need to adapt to implement the solutions that respond to the challenge addressed by the foresighting cycle.

Typically, organisational changes will also require the adoption of new capabilities and a change in the distribution of these capabilities across supply chain partners. The change in capabilities within an organisation as well as their supply chain partners will determine the changes knowledge and skill changes required by the role groups within the workforce of each supply chain partner.

Step Two – How will the Workforce change - Occupational Changes

A set of Future Occupational Profiles (FOPs) is produced by the foresight process that demonstrates how current occupations may need to change in the future. FOPs are generated using a combination of attributes from the underlying capability classification and from data collected in multistakeholder workshops. The FOP generation algorithm works to group logical sets reflecting similarity of role levels, function, proficiency, and capability.

As part of the foresight process the generated FOPs are reviewed, revised and distilled by the Employer group. The agreed set of FOPs are then compared with selected current education provision; the default reference is the set of Institute for Apprenticeships and Technical Education (IfATE) apprenticeship standards; to assess which current training and education provision could be used in the future. Two bespoke metrics – match and surplus[3] – are used to evaluate the alignment of current provision with the set of FOPs proposed. Summaries are presented of the key findings related to each Supply Chain partner.

Findings and insights outlined in this section are aimed at both Employers, and Education and Training Providers, and identify matches and gaps in future training needs compared with current provision to guide further detailed investigation.

[3] A definition for match and surplus is brought forward in Section 3.4.

Step Three – How the current Education provision meets the future need - Highlighted Changes to Future Provision

The report identifies suggested changes to education and training provision – principally apprenticeship standards that will deliver the knowledge, skills and behaviours required by future occupations. In some cases, this will include the development of short courses and continued professional development (CPD) to upskill the current workforce to meet future needs. Additionally, foresighting outputs can be used to develop programmes, qualifications, and apprenticeship standards for new entrants to the workforce joining via apprenticeship, taught qualification, or other training programme.

The insight and data in this part of the report are primarily aimed at educators training providers, apprenticeship standards bodies and awarding organisations. Combined with insight arising from the Supply Chain capability changes, the provision insight offers an effective way for employers to identify training opportunities that align to their future needs.

3.2 Step One – How will the Supply Chain change - Organisational Changes Insight

Organisation functional area

The Workforce Foresighting process uses an information architecture built on five functional areas which are common to any business:

Design	The function of an organisation that focuses on activities relating to product, service, or solution design.
Implement	The function of an organisation that focuses on activities relating to producing / making / providing its products or services.
Logistics	The function of an organisation that focuses on activities relating to procurement, delivery, materials, or services necessary for operations – service / manufacturing, etc.
Support	The function of an organisation that focuses on activities relating to users, in-service support, repair / maintenance, recycling, end of life disposal.
Enterprise	Core functions of an organisation - e.g., strategic planning, leadership and management, human resources, digital backbone and data systems, integration of relevant statutory / regulatory requirements and compliance.

The functional structure is developed to levels of detail that enable the foresight process to reference external data sets including ONET (US) Occupational Information Network [9F[4]],

[4] ONET - Occupational Information Network - https://www.onetcenter.org/

ESCO – European Skills, Competences, Qualifications and Occupations1[5], IfATE (UK) Institute for Apprenticeships and Technical Education[6].

The five organisation functional areas comprise around 40 domains which are broken down to around 140 functional areas. The architecture is used to position ~25,000 capability statements we developed during the Cycle which are the building blocks used in the workforce foresight process. Each capability statement has several attributes – some are static and reflect the position of the capability statement in the architecture, whilst others are dynamic and are assigned values through a cycle and set of workshops.

The data architecture is implemented in a bespoke ‘data-cube’ which underpins the foresight process, workshops, and enables extensive use of LLM and AI tools. Additionally, a key feature of the data-cube is that the data from each foresight topic cycle is added into the data set and can then be used, where relevant, in future cycles. This ensures that the capabilities of the system are dynamic and up to date.

Identifying the Future Supply Chain Capabilities

The diagrams presented in this analysis depict how the supply chain’s capabilities are expected to evolve in the future. Drawing on insights from three workshops with Technologists, the following pie chart illustrates the distribution of skills across five distinct functions, with current data anchored in apprenticeship standards from existing supply chain partners providing a comparative baseline. Although the present information is less detailed than the workshop findings, it is a valuable reference point for understanding emerging trends.

[5] ESCO - European Skills, Competences, Qualifications and Occupations - https://esco.ec.europa.eu/en
[6] IfATE – Institute for Apprenticeships and Technical Education - https://www.instituteforapprenticeships.org/

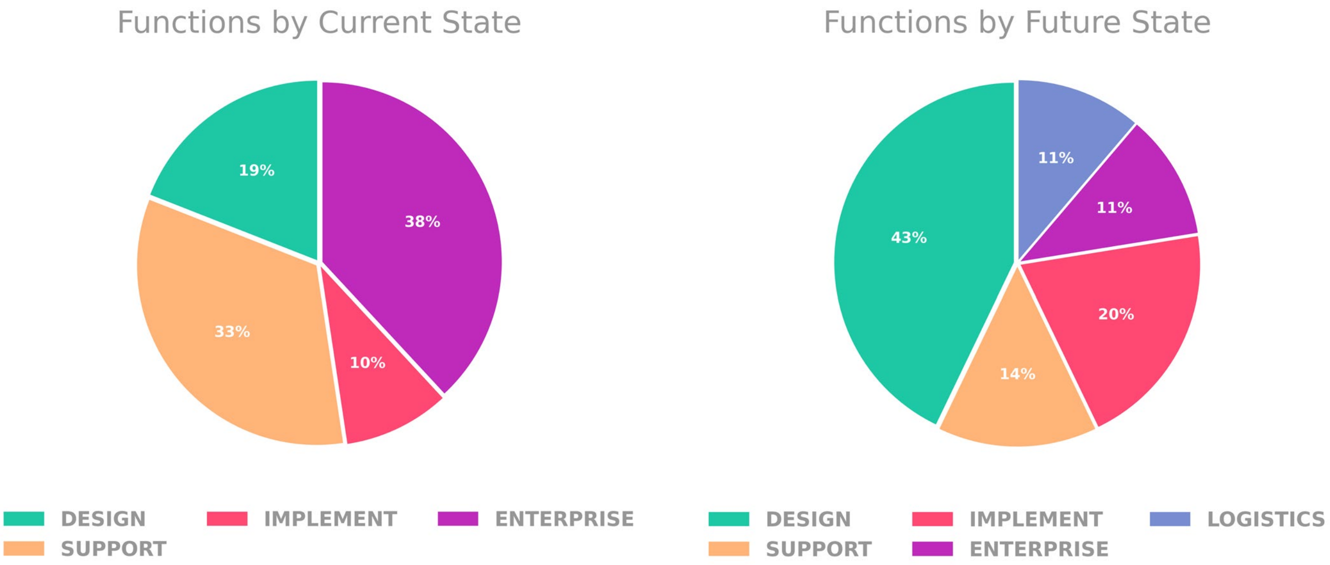


Figure 3: Current and Future – Whole Supply Chain - Capability Function Distribution %

A closer look at the data reveals a shift in emphasis among these functions. The Design role, for instance, is forecast to experience a significant surge, expanding from 19% to 43% and positioning itself as the foremost area of focus. In contrast, the Enterprise function is expected to contract markedly, declining from 38% to 11%, a change that suggests a move toward greater efficiency or increased automation. The Support function, too, is expected to diminish in relative importance, with its share reducing from 33% to 14%. Meanwhile, the Implementation function is poised to grow from 10% to 20%, reflecting the heightened demands of new projects and advanced technologies. Additionally, Logistics emerges as a notable new element, accounting for 11% of the future capabilities and signalling evolving operational priorities.

While these insights into current and future capabilities illuminate significant relative changes, it is also clear that the overall impact will depend on the volume of activity within each function.

Design Domains

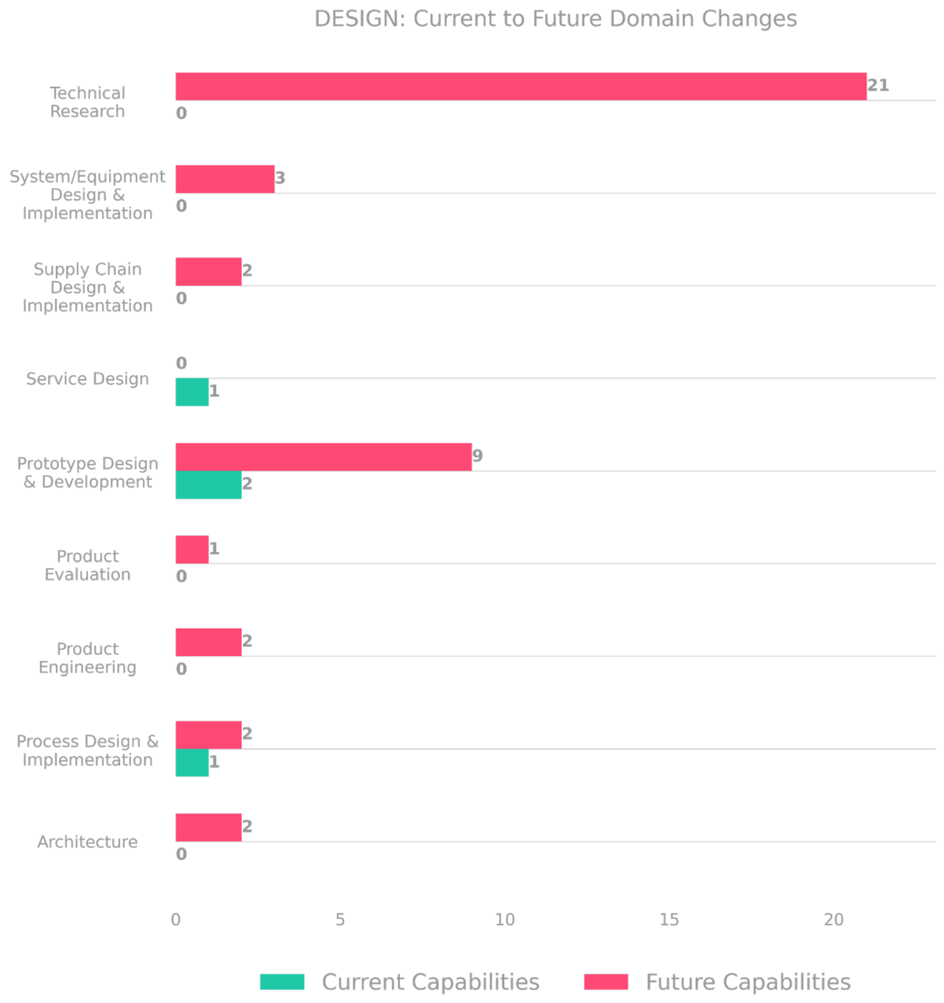


Figure 4: Design Future Domain Spread of Capabilities

The design function emerges as the most robust area, representing 46 of the 131 organisational capabilities identified for this cycle. At the domain level, the strongest concentration of capabilities is found within process design and implementation, where the focus is on modelling and developing processes. Following this, prototype design and development takes a close second, emphasising creating systems and applications rather than traditional physical prototypes.

The comparison between the current and future states highlights a strategic shift. There is a clear move toward frontloading innovation in the coming period – in other words, focusing on developing new products, engineering, and evaluation well before the development and implementation phase. This realignment is evident in the expansion of technical research, which grows from zero to 21 capabilities, reflecting a robust commitment to research-driven innovation.

Equally, the rise in prototype design and development from two to nine capabilities points to the increasing importance of iterative design and testing. The emergence of system and equipment design and implementation, which moves from zero to three capabilities, further reinforces the emphasis on integrating new systems. In parallel, enhancements in supply chain design and implementation, product evaluation, and product engineering – each starting from zero and growing modestly – suggest a diversified approach to innovation. Additionally, there is a moderate increase in process design and implementation and the introduction of architectural capabilities, which signals a focus on high-level system design.

Enterprise Domains

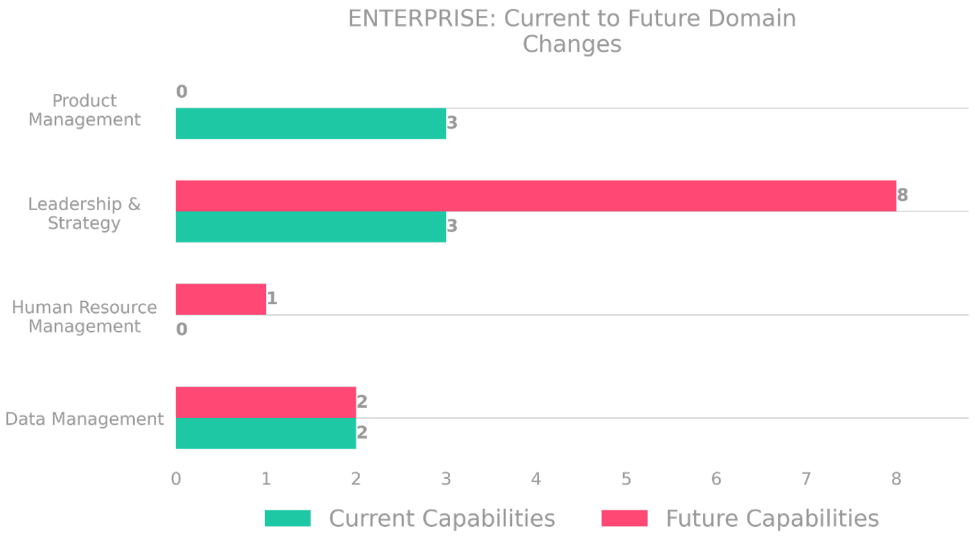


Figure 1: Enterprise Future Domain Spread of Capabilities

The enterprise function is the second most prominent area, with 31 out of 131 capabilities, stressing a well-defined focus on supporting the business from multiple strategic angles. Many of these capabilities are anchored in Data Management, where organisations concentrate on the technical aspects of performing data analysis, designing secure and efficient storage solutions, and rigorously evaluating data quality.

In parallel, there is a clear emphasis on leadership and strategy, with efforts geared toward identifying new business partnerships, assessing emerging threats and opportunities, and gauging the environmental impact of strategic decisions. This function also integrates regulatory compliance by coordinating activities and keeping abreast of changing regulations, reflecting its role in maintaining operational integrity.

The evolution from current to future capabilities in the enterprise domain mirrors the broader market dynamics of a maturing and competitive regulated environment, where the need to support human resource capacity is becoming increasingly pronounced. Detailed comparisons at the domain level reveal that leadership and strategy capabilities have notably expanded from three to eight, spotlighting a growing reliance on strategic direction and decision-making.

Meanwhile, human resource management, previously absent, emerges as a new priority, signalling an essential focus on workforce development and talent management. In contrast, product management has been entirely phased out, a shift that suggests a reduced emphasis on overseeing the product lifecycle. Data management remains a stable and indispensable component throughout these changes, retaining its established role within the enterprise framework.

Implementation Domains

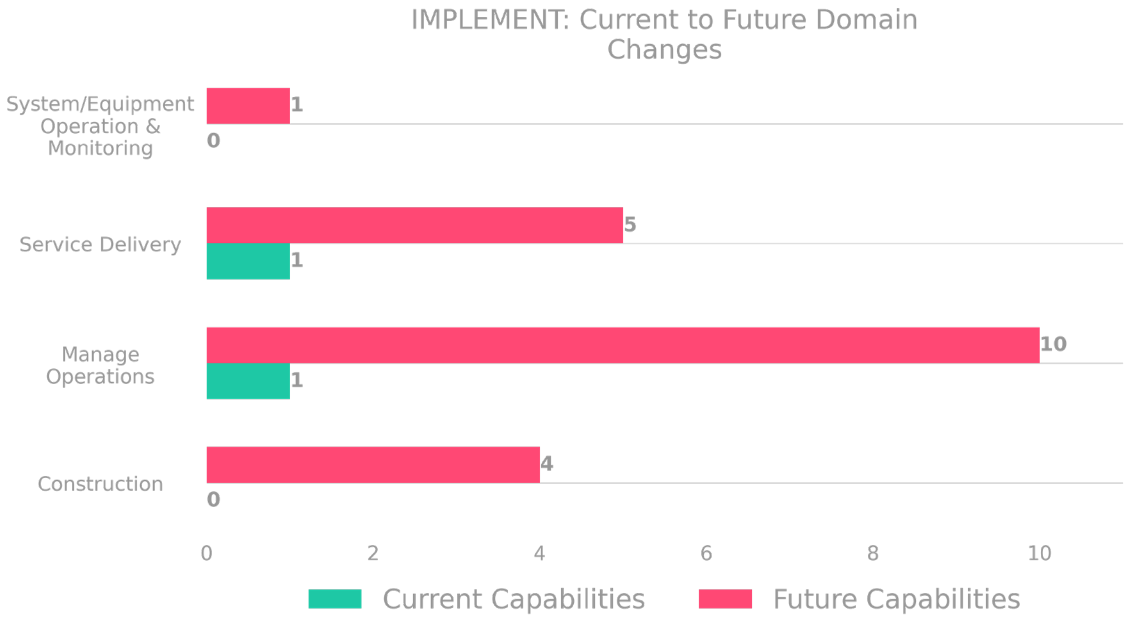


Figure 2: Implementation Future Domains Spread of Capabilities

Among the 131 capabilities identified for this cycle, 28 fall under the implement function, with a predominant focus on operational management and service delivery. This area covers a range of activities, from creating and processing digital data to analysing and verifying information, as well as planning, scheduling, communicating, and translating critical information. In addition to these functions, there is also a notable presence of capabilities devoted to monitoring systems and equipment and managing operations.

Examining the domain-level shifts within the implement function reveals a clear prioritisation of operational management and practical execution. The capability for managing operations shows the most striking growth, from one to ten, underscoring an emerging emphasis on robust operational oversight and efficiency. Service delivery, too, is expected to expand, growing from one to five capabilities, indicating a deliberate focus on ensuring high-quality service execution.

The data also highlights the introduction of construction as a new capability, rising from zero to four, which reflects an increasing need for infrastructure-related skills. Moreover, system and equipment operation and monitoring, newly introduced with an increase from zero to one, signals a commitment to sustaining real-time system performance and proactive maintenance.

Logistics Domains

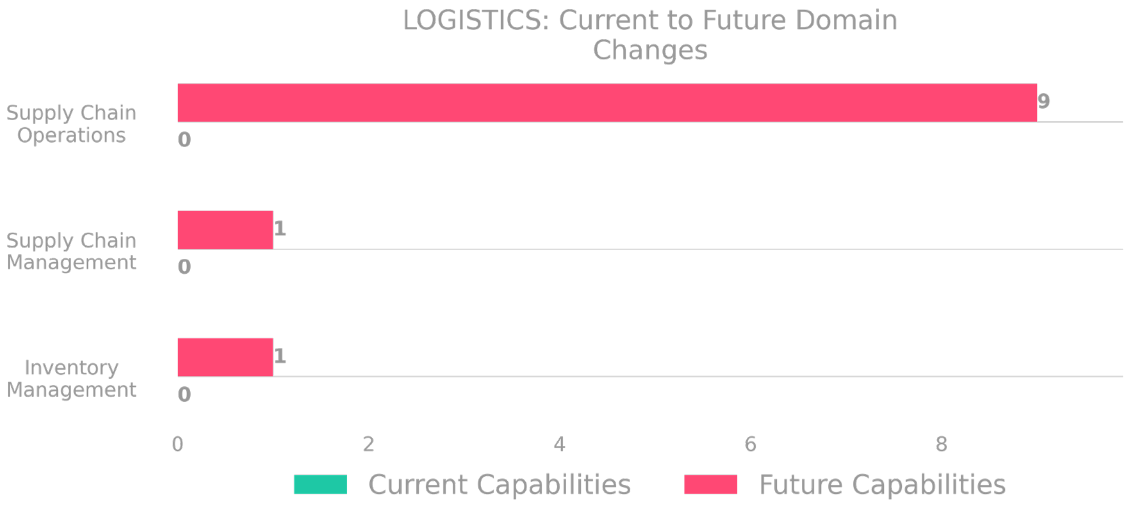


Figure 3: Logistics Future Domains- Future Spread of Capabilities

The logistics function is notably modest within the 131 capabilities identified for this cycle, with only eleven capabilities in place. These capabilities are distributed across critical areas such as identifying and collaborating with suppliers, monitoring inventories, coordinating the flow of inventory, and managing transport services. As organisations prepare to scale up the planning and deployment of digital twins, the comparison between current and future logistics states reflects an anticipated operational scale evolution. A closer examination of the domain-level changes reveals that supply chain operations experience the most dramatic expansion, growing from zero to nine capabilities. This signifies an enhanced focus on ensuring the supply chain is compliant with the stringent cyber-physical security demands of the Sector.

Additionally, supply chain management emerges with a new capability, pointing to the increasing necessity for strategic oversight. Further, inventory management is introduced, a shift toward improved input control and resource optimisation.

Support Domains

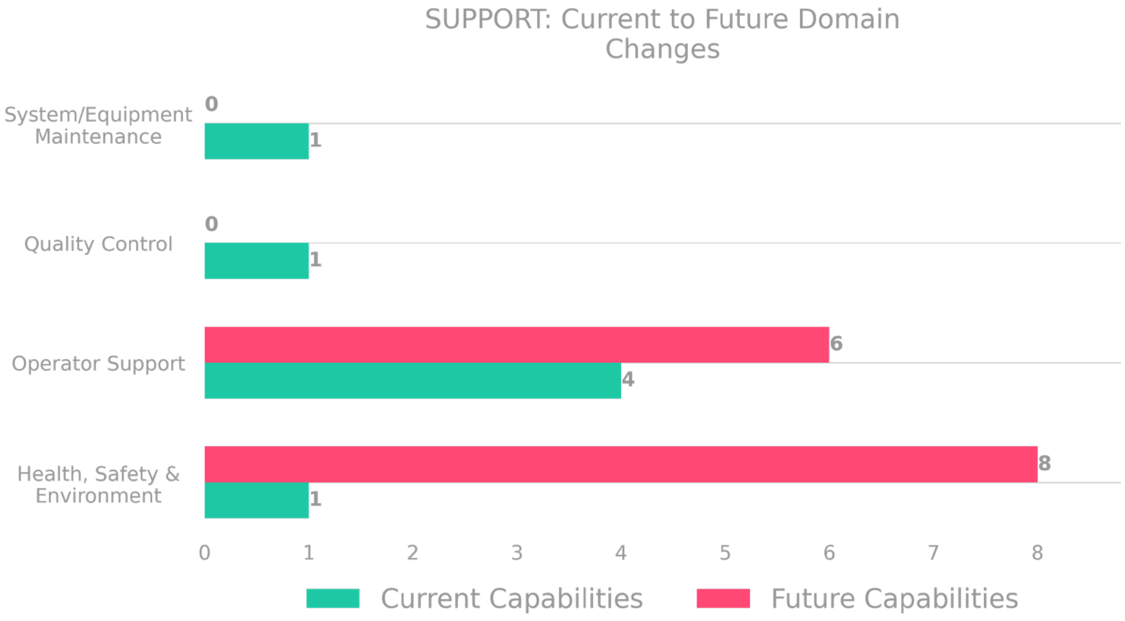


Figure 4: Support Future Domains - Future Spread of Capabilities

Within the 131 capabilities identified for this cycle, the support function accounts for 14. A closer examination at the domain level reveals significant shifts within the support function. Notably, the Health, Safety & Environment capability experiences a robust increase, rising from a single capability to eight, which signals an intensified focus on workplace safety, regulatory compliance, and environmental considerations. In parallel, Operator Support expands modestly from four to six capabilities, reflecting an ongoing commitment to empowering and assisting field workers in an increasingly complex operational environment. Conversely, traditional roles such as System/Equipment Maintenance and Quality Control are phased out entirely, dropping from one capability each to none, which suggests a deliberate move away from in-house maintenance and dedicated quality assurance functions - possibly a consequence of greater reliance on automation, outsourcing, or improved processes.

Visualisation Instructions

Detailed instructions can be found in the appendix.

Visualisation Data Link	**What is it and what can it be used for?**
Organisational Capabilities	*The page provides details of the capabilities required by each supply chain partner and the supply chain as whole. The information is presented using the Capability Classification Framework , Design / Implement / Logistics / Support / Enterprise and can be interrogated and then exported to suit specific user requirements and interest.* *The information provided also identifies capabilities supported by existing provision, and also where there may be gaps that require new development to support to equip the future workforce.*

3.3 Step Two – How will the Workforce change - Occupational Change Insight

Insight into occupational change uses the understanding of how capabilities will change across business functions (section 3.2) to inform proposals for how occupations and their associated skills sets for each supply chain partner may need be revised to reflect change for each role level within that partner.

Supply Chain partner organisation types

The workforce foresighting process recognises that different partners in a Supply Chain will require appropriate capabilities, and these are determined and agreed in the initial workshops.

In this cycle, the following Supply Chain partners were identified and then used during participant workshops and data analysis to determine the organisational needs:

1. Research and Development Organisations
2. Software Development Companies / Suppliers
3. Systems Integration Specialists & Consultants
4. Transport Operators
5. National Cyber Security Centre
6. Regulators and Auditors

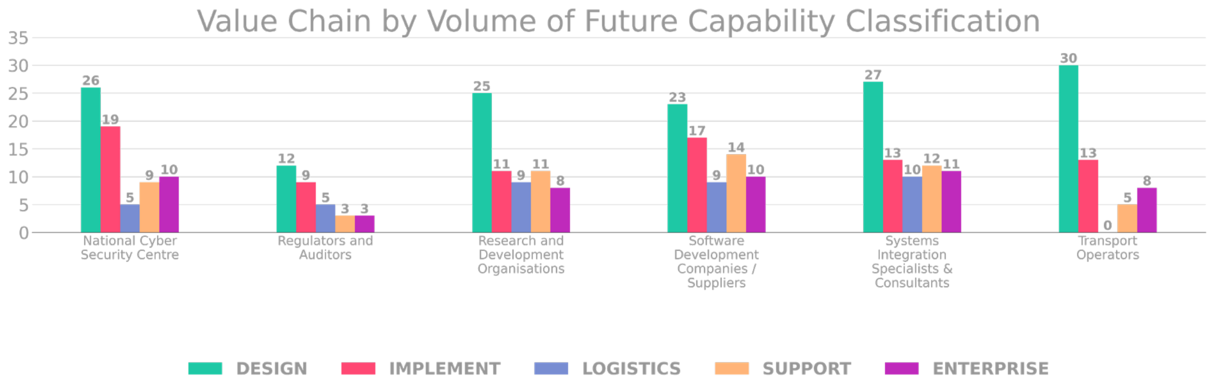


Figure 5: Distribution of Functions across each Supply Chain Partner

The graph illustrates the distribution of capabilities across various functions among Supply Chain Partners, forming the foundation for Future Occupational Profiles (FOPs) at each role level. It clearly shows how future capabilities are distributed along the value chain, with a noticeable concentration in specific areas. Design and Implementation functions overwhelmingly dominate the landscape, suggesting that innovation, technical research, and system development will be the primary drivers of future growth. In contrast, the Enterprise, Logistics, and Support functions occupy a smaller share, reflecting their more specialised roles in the broader operational framework.

Visualisation Instructions

Detailed instructions can be found in the appendix.

Visualisation Data Link	**What is it and what can it be used for?**
Supply Chain Capabilities	*This page provides an overview of the identified capabilities at a Supply Chain Partner level.* *By selecting/deselecting each Supply Chain Partner you can review the capabilities identified as required in that area of the Supply Chain.* *This can be used to generate organisational capability profiles for each area of the Supply Chain to help prioritise and focus the acquisition of new capabilities that will be required in the future.* *It can also be used to generate combined organisational profiles, where an organisation may be involved in more than one area of the Supply Chain.*

Role Levels

The foresighting process uses the concept of Role Levels to represent future occupations. Utilising this approach acknowledges that the workforce is not homogeneous, there will be varying levels of proficiency required across a workforce and qualifications and training may be aligned/require different types of vocational or academic qualifications. Additionally, the role level approach seeks to avoid presuming that the future workforce will be operating at a different level to the current state. Finally, we acknowledge that Role Levels and Titles may vary based on the organisation implementing them.

Role Levels determined through workshops:

Role Seniority	Role Title	Role Description
Senior	Senior Research Scientist (Simulation)	Leading the development of digital twin-based security simulations.
	Senior Cybersecurity Innovation Lead	Driving the strategic integration of digital twin technology into cybersecurity operations.
	Senior Compliance Officer (Simulation)	Ensuring regulatory alignment of digital twin-based security practices.
	Senior Cybersecurity Auditor	Evaluating digital twin applications for compliance with cybersecurity standards.
	Senior Digital Twin Specialist	Overseeing the deployment and iterative refinement of digital twin models for security testing.
Mid-level	Prototyping Engineer	Developing proof-of-concept digital twin security models.
	Software Developer	Creating simulation environments for cyber-physical security testing.
	Cybersecurity Specialist	Managing digital twin-enabled threat modelling and response strategies.
	BIM Specialist	Integrating Building Information Modelling (BIM) with digital twin security solutions.
	Systems Integration Specialist	Ensuring the integration of digital twins within OT/IT security frameworks.
	Cybersecurity Consultant	Advising on best practices for digital twin-enabled cybersecurity.
	Compliance Officer	Aligning digital twin applications with regulatory security requirements.
	Digital Twin Specialist	Managing digital twin models for security simulations and predictive maintenance.
	Simulation Engineer	Designing and testing cyber-physical threat scenarios within digital twin environments.
	Project Manager	Overseeing the implementation of digital twin cybersecurity initiatives.
	Software Test Engineer	Validating digital twin applications for cybersecurity resilience.
Junior	Digital Twin Engineer	Assisting in the deployment and maintenance of digital twin security solutions.
	Data Analyst	Analysing threat data generated by digital twin simulations to identify vulnerabilities.

Proficiencies

Each of these role levels will require proficiency that reflects their role and the needs of each Supply Chain Partner. The foresight process uses a three-point scale to capture and differentiate the proficiencies required. This information is used both in the generation of the FOPs, and to assist the definition of training needs identified. Within the workforce foresight process proficiency is defined as:

Awareness (A) – Has a foundational knowledge of tools, technology, techniques relevant to sector, industry, or organisation. Sufficient comprehension to know where to seek further information/details as necessary for a particular issue.

Practitioner (P) – Has the ability to apply and use independently a tool, system, or process. Understands the implications, consequences, and impact for their role/function. A Practitioner knows what key actions are required and in what context.

Expert (E) – Has detailed knowledge of process, system, tool, or technology. Can support others and identify improvements required for a process, system, or tool. An Expert can implement improvements personally or direct and guide others.

During the workshops participants applied their insight to assign proficiency for each role group to each capability. Individual responses were aggregated by the system to arrive at a consensus.

A summary of the distribution of required proficiency for the role levels in this cycle are:

	Junior Level	**Mid-Level**	**Senior Level**
Awareness	0	0	2
Practitioner	48	123	53
Expert	13	84	79

The data clearly shows that most workforce capabilities are designed for roles that require more than just a basic level of understanding. Many capabilities demand Practitioner-level expertise, with 123 instances identified at the mid-level, highlighting the need for applied skills in everyday operations. Additionally, Expert-level capabilities are substantial, with 84 capabilities at the mid-level and 79 at the senior level, which underscores the industry’s call for advanced knowledge and specialised proficiency. Minimal emphasis is placed on foundational awareness, suggesting that the future workforce will predominantly engage in roles that require hands-on application and a deep mastery of their craft.

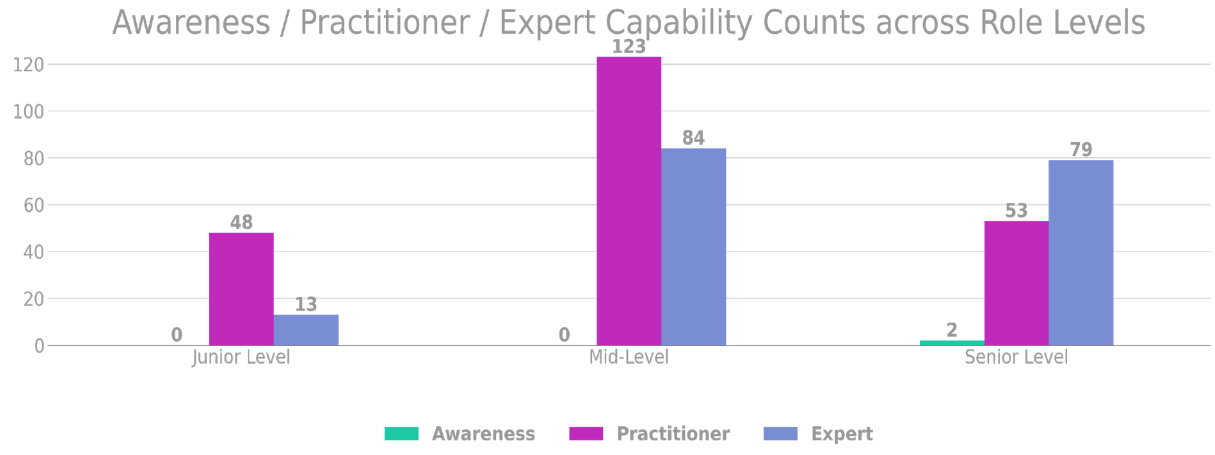


Figure 6: Proficiency details by Role Level

Future Occupational Profiles (FOPs)

FOPs are used to describe and suggest occupations, or roles, that may be required in the future and provide a framework to indicate capabilities and related duties. They can be used to review the impact on current roles and the adaptation that may be required in the future.

Educators can review current apprenticeship standards against the requirements of the FOPs and interpret which need to be changed to fill the gaps between the current and future state.

Employers can consider existing apprenticeship standards and make a judgement on adapting an existing apprenticeship standard to upskill their workforce to meet the requirements of a particular FOP.

FOPs and indicative skills need

Combining proficiency with the identified FOPs, the following graphs indicate the priority needs across the supply chain for each Role Group to deliver future capabilities.

Junior Level Role Level FOPs:

In this cycle the Junior Level role level was defined as occupations and roles requiring Level 2 qualifications or apprenticeships.

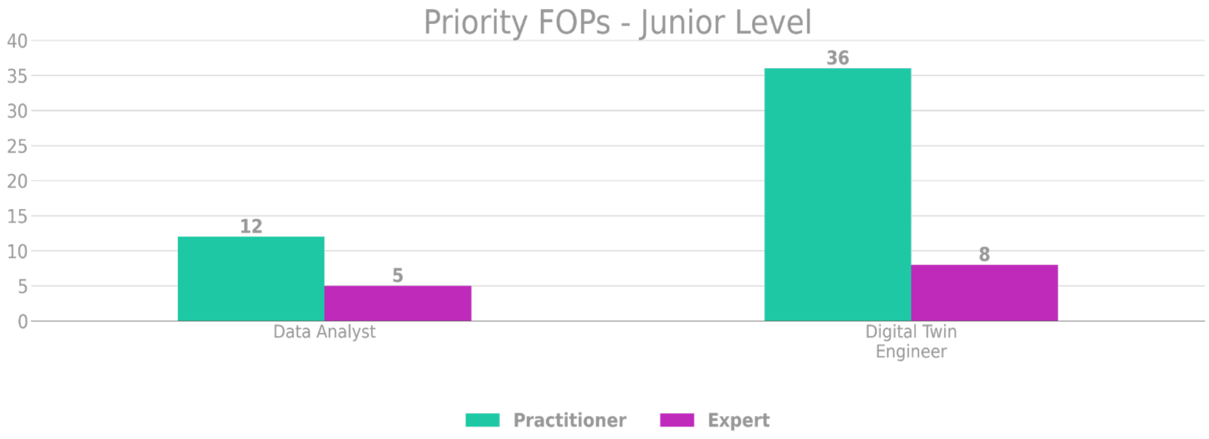


Figure 10: Priority FOPs - Junior Level Role Level

Mid-Level Role Level FOPs:

In this cycle the Mid-Level role level was defined as occupations and roles requiring Level 4 qualifications or apprenticeships.

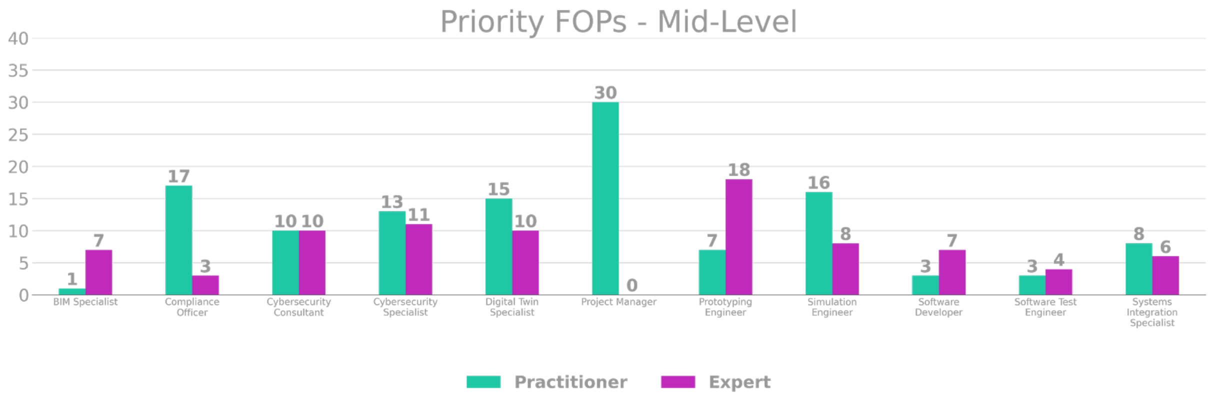


Figure 11: Priority FOPs - Mid-Level Role Level

Senior Level Role Level FOPs:

In this cycle the Senior Level role level was defined as occupations and roles requiring Level 5 qualifications or apprenticeships.

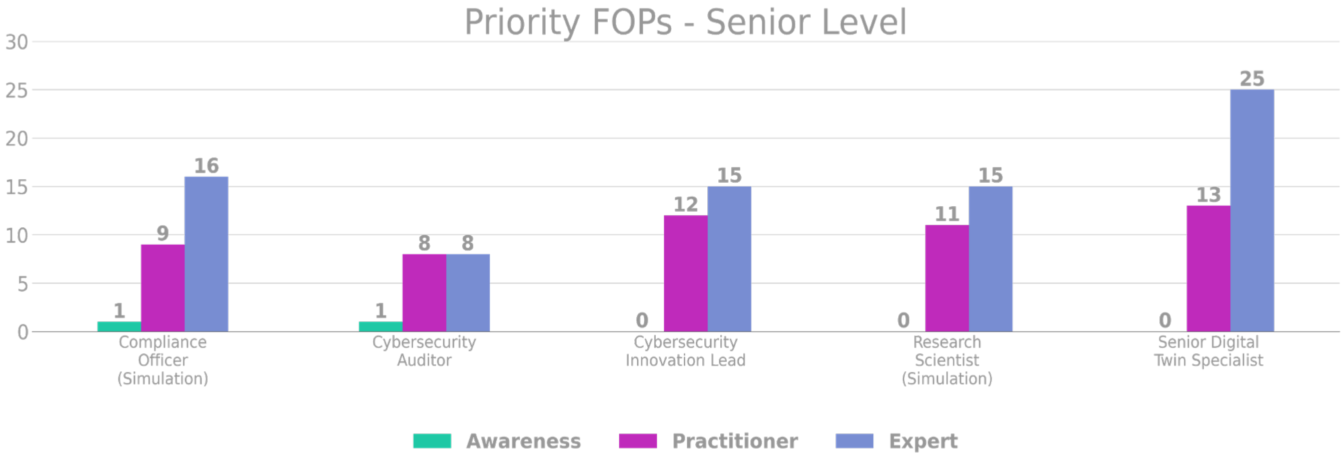


Figure 12: Priority FOPs - Senior Level Role Level

Visualisation Instructions

Detailed instructions can be found in the appendix.

Visualisation Data Link	What is it and what can it be used for?
FOP Matrix	*This page provides a detailed breakdown of future occupational profiles that could be required in the future workforce. These were generated using a combination of attributes collected through the workshops and an algorithm. These suggested profiles were then reviewed and ratified by small groups of employers who were able to add/remove capabilities and uprate/downrate proficiency levels required.* *You can view all the FOPs in a role level by selecting one (or more) of these from the drop down. This will then allow you to select the FOPs aligned to that role level.* *The populated table allows you review and compare different FOPs within or across role levels. You can view the capabilities in each FOP and the assigned proficiency levels.*

3.4 Step Three – How the current Education provision meets the future need – Highlighted Changes for Future Provision

The Workforce Foresighting process has developed two metrics to quantify the alignment between a FOP and a current standard or qualification:

> **Fit** – expressed as a %, it is a measure of the proportion of a FOP that is covered by an existing standard or qualification.
>
> **Surplus** – expressed as a %, it is a measure of the not relevant material in an existing standard that is not required for a FOP.

An ideal existing qualification or standard would have a high fit and low surplus – this implies good coverage of the FOP but with little material that is not relevant to the FOP. Conversely a poor candidate would have a low fit and high surplus. Using these two metrics it is possible to quantitively evaluate, rank, and compare a range of existing training provisions against a set of FOPs describing future needs.

Our interpretation is represented by a simple nine-box model to position the suitability of a given current occupational standard to a future occupational profile:

Factor scores

Fit Factor	Fit score	Surplus Factor	Surplus score
0 - 32%	1	81-100%	1
33-65%	2	51-80%	2
66-100%	3	0 - 50%	3

(Multiplying the Fit score by the Surplus score gives a Suitability Grid score of 1-9 below)

Suitability Grid

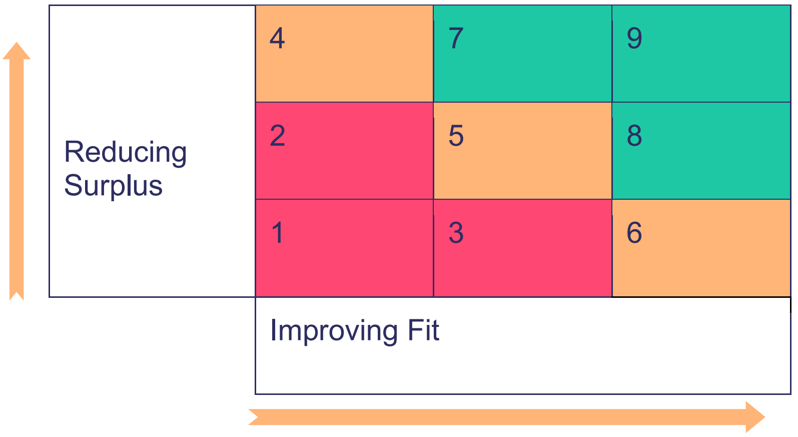


Figure 7: Fit Factor scores and Suitability Grid

Using this score and indicated ‘RAG status’ the following interpretations can be made:

High Suitability – 7,8,9 – for standards that have good coverage of FOPs.

Represents good candidates from current apprenticeship standards used as the basis of development to meet FOP requirements and inform elements of short course and CPD provision.

Some Suitability– 4,5,6 – for standards that have only partial coverage of FOPs.

These are likely to require extended work to meet FOP requirements, further review of the data may be necessary. They are likely to contain some useful information to inform elements of short course and CPD provision.

Low Suitability – 1,2,3 – for standards that have poor coverage of FOPs.

These are unlikely to be adaptable to meet future needs but may contain some useful information to inform elements of short course and CPD provision, which can be assessed using the data visualisation tools.

FOP findings compared with current standards

Using the approach described above and applying the 'RAG' scores to each FOP indicating the suitability of current apprenticeship standards selected from the IfATE set, the following table begins to identify areas of action and concern for the provision of future skills for each Supply Chain Partner to respond to the challenge. This high-level suitability summary compares the best matching current IfATE qualifications or apprenticeship standards and gives the current suitability in the following table.

Supply Chain Partner - Research and Development Organisations

Role Level	Selected Future Occupational Profiles	Current Suitability Summary
Senior Level	Research Scientist (Simulation)	Some
Senior Level	Cybersecurity Innovation Lead	Low
Mid-Level	Software Test Engineer	Low
Mid-Level	Prototyping Engineer	Some

Detailed breakdown:

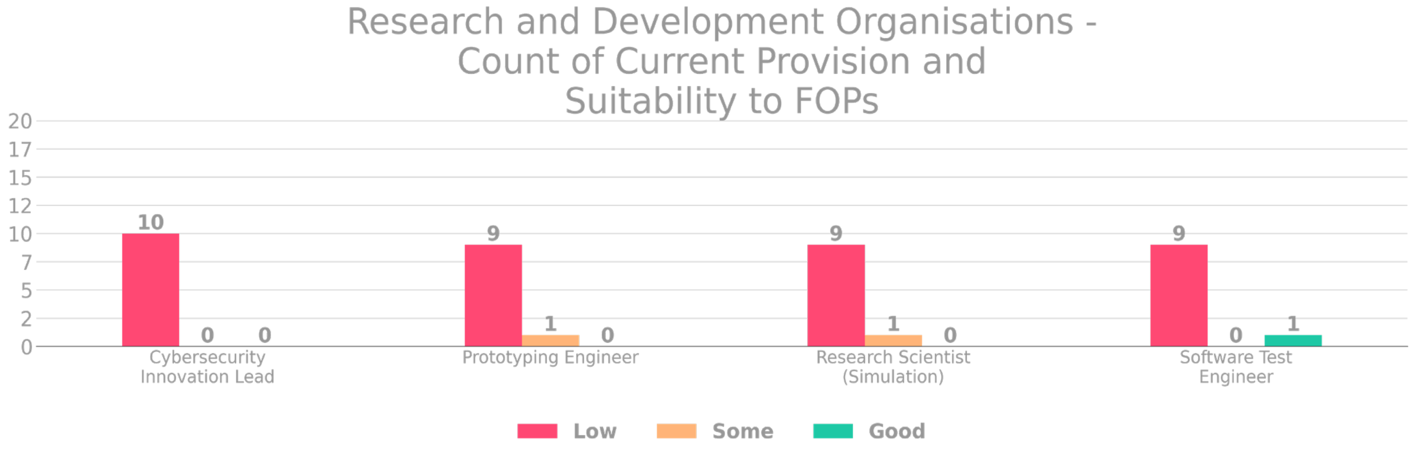


Figure 14: Suitability Summary - Research and Development Organisations

Supply Chain Partner - Software Development Companies / Suppliers

Role Level	Selected Future Occupational Profiles	Current Suitability Summary
Mid-Level	Cybersecurity Specialist	Some
Mid-Level	BIM Specialist	Low
Mid-Level	Software Developer	Low
Mid-Level	Project Manager	Some
Junior Level	Data Analyst	Some
Junior Level	Digital Twin Engineer	Low

Detailed breakdown:

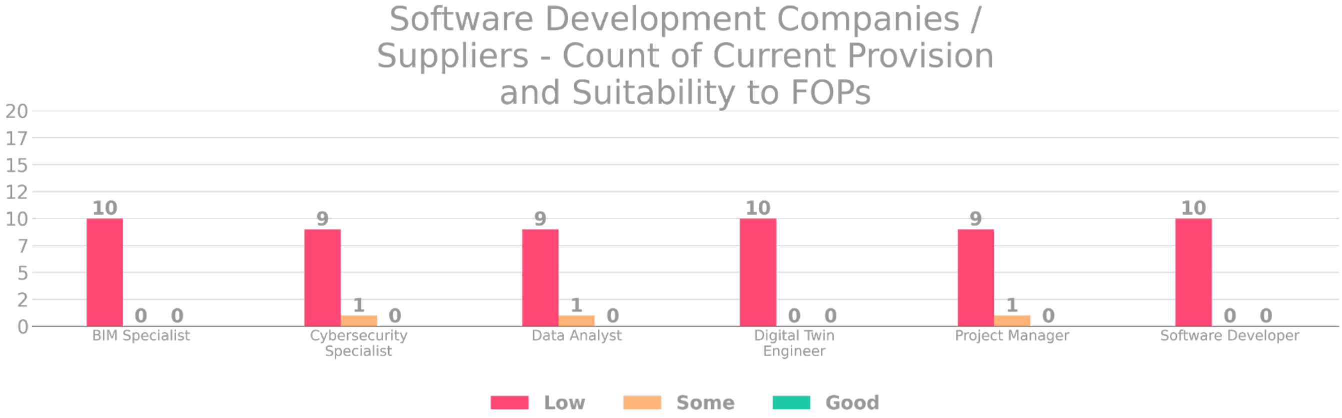


Figure 15: Suitability Summary - Software Development Companies / Suppliers

Supply Chain Partner - Systems Integration Specialists & Consultants

Role Level	Selected Future Occupational Profiles	Current Suitability Summary
Mid-Level	Cybersecurity Consultant	Some
Mid-Level	Project Manager	Some
Mid-Level	Systems Integration Specialist	Low
Junior Level	Digital Twin Engineer	Low

Detailed breakdown:

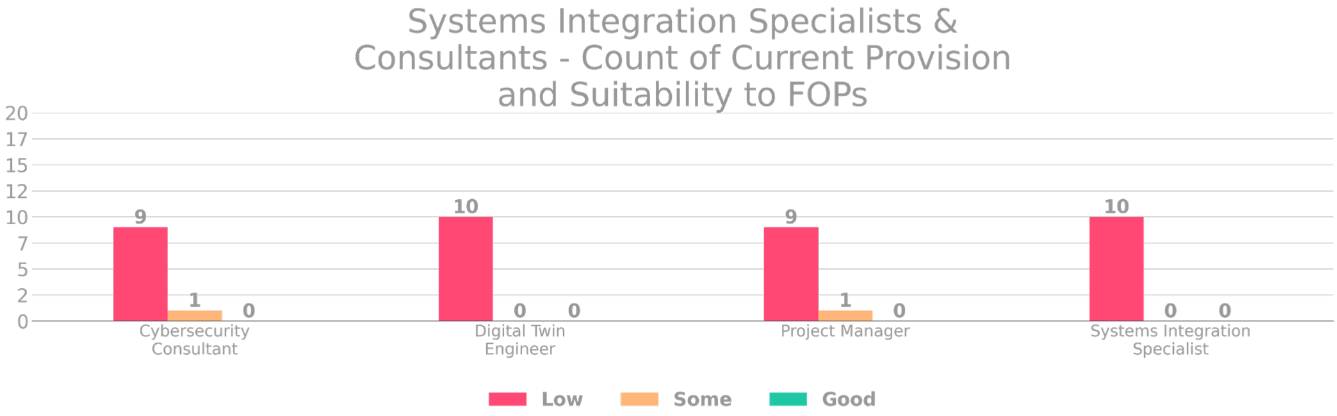


Figure 16: Suitability Summary - Systems Integration Specialists & Consultants

Supply Chain Partner - Transport Operators

Role Level	Selected Future Occupational Profiles	Current Suitability Summary
Senior Level	Cybersecurity Innovation Lead	Low
Mid-Level	Compliance Officer	Some
Mid-Level	Prototyping Engineer	Some
Mid-Level	Project Manager	Some
Mid-Level	Software Test Engineer	Good
Junior Level	Data Analyst	Some

Detailed breakdown:

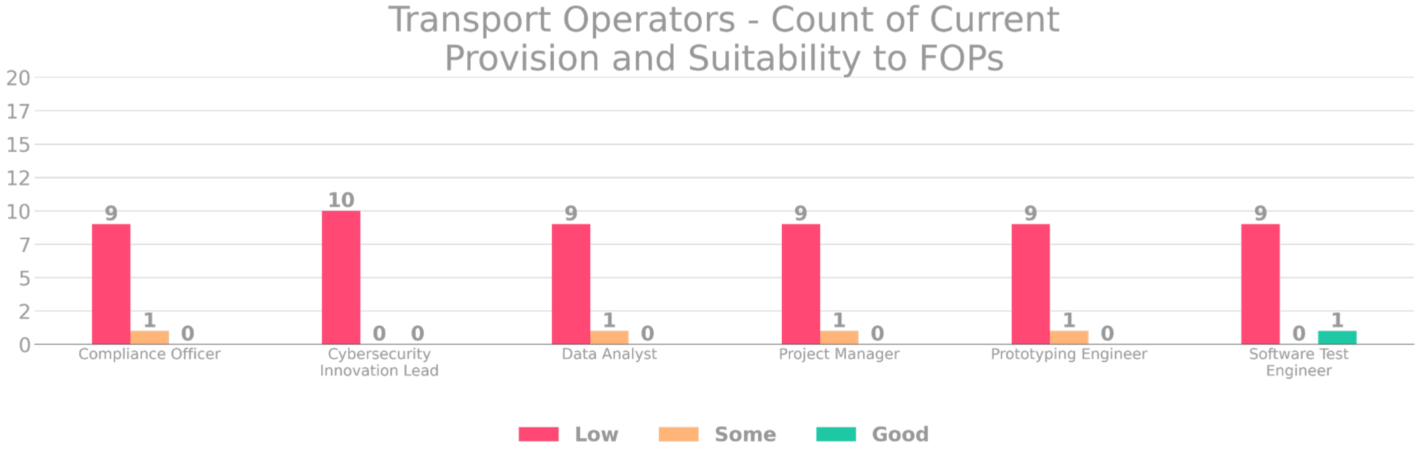


Figure 17: Suitability Summary - Transport Operators

Supply Chain Partner - National Cyber Security Centre

Role Level	Selected Future Occupational Profiles	Current Suitability Summary
Senior Level	Compliance Officer (Simulation)	Low
Senior Level	Cybersecurity Auditor	Low
Senior Level	Senior Digital Twin Specialist	Low
Mid-Level	Compliance Officer	Some
Mid-Level	Simulation Engineer	Low
Mid-Level	Digital Twin Specialist	Low

Detailed breakdown:

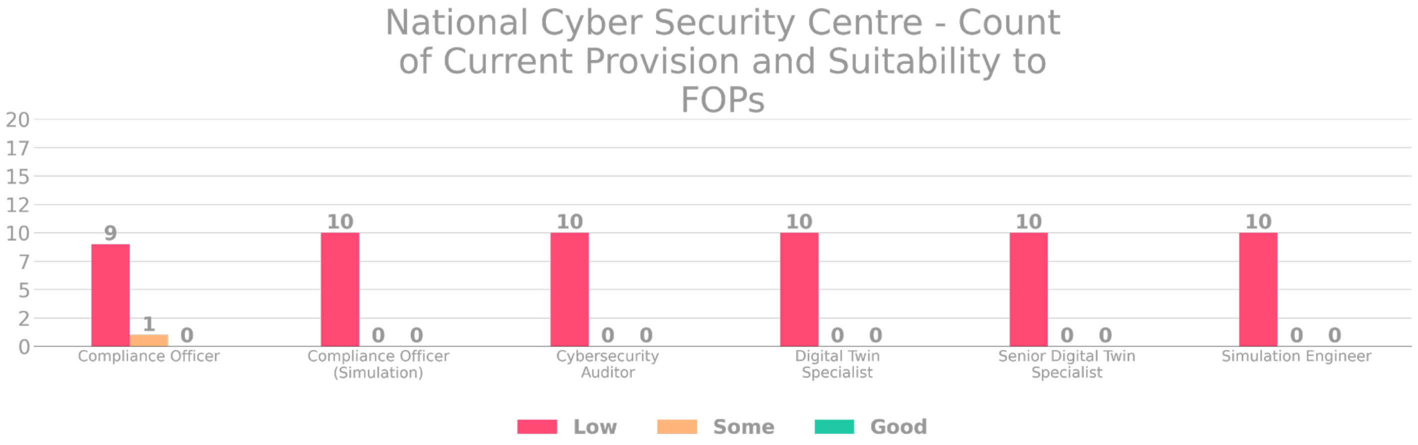


Figure 18: Suitability Summary - National Cyber Security Centre

Supply Chain Partner - Regulators and Auditors

Role Level	Selected Future Occupational Profiles	Current Suitability Summary
Senior Level	Compliance Officer (Simulation)	Low
Senior Leve	Cybersecurity Auditor	Low
Senior Level	Senior Digital Twin Specialist	Low
Mid-Level	Digital Twin Specialist	Low

Detailed breakdown:

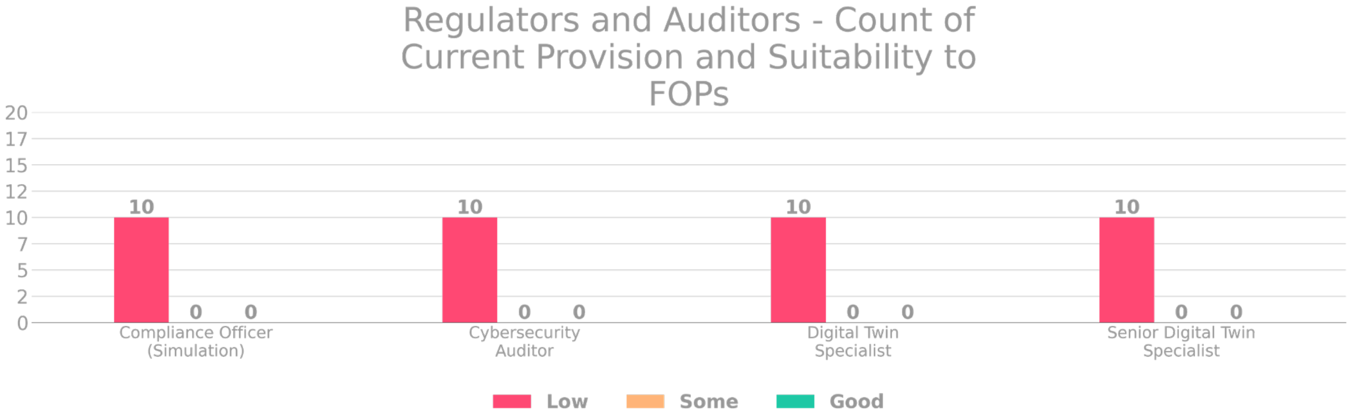


Figure 19: Suitability Summary - Regulators and Auditors

Link to full data set - Visualisation Instructions

Visualisation Data Link	What is it and what can it be used for?
FOP Detail	*This page allows you to review a specific Occupational Profile, including the capabilities contained within it and the Knowledge, Skills & Behaviour (KSB) tags associated with the capability.* *You can select an individual Role Level and linked FOP in the two available dropdowns. The table in the lower section of the page will then be populated with all relevant capabilities.* *The search control above the table allows you to filter content of any of the columns of data. A key piece of functionality in this table is the presence of the KSB tags associated with the capabilities.*
Future KSBs Summary	*This page provides a view of the complete set of capabilities within the cycle along with all of the associated KSB tags which are linked to them. It is, essentially, the superset of all details displayed on the Fop_detail page.* *This is used to:* • *To review the identified Knowledge, Skill and Behaviour tags for a given capability, to support development of future education and learning material.* • *To review the requirements from a capability level, rather than a role level/occupational profile grouping.*
Capabilities Matched to Current Provision	*This page allows you to review and compare individual capabilities against 'Duty' statements in an Apprenticeship / Occupational Standard.* *You can select individual capabilities to review their specific matches. These matches are shown in the bottom panel, including the Standard, the Level and the Duty Statement this is matched to.* *You can filter in several ways to focus your review:* • *By the Capability Classification Framework (left-hand panel).* • *By capabilities that **are** served by the reference mapping framework – the default is Institute for Apprenticeships and Technical Education (IfATE) provision.* • *By capabilities that **are not** served by the reference mapping framework, e.g., IfATE provision – these are capabilities required in the future that may require new/bespoke training and CPD materials to be developed to upskill/re-skill the workforce.* *This page can be used to identify where existing provision may exist across the broad spectrum of Apprenticeship standards, and not just within a narrow range of sector-specific Standards.* *The data also allows you to identify where provision may already exist to support specific capabilities.*

Fit & Surplus Factors	*This page allows you to review the 'Fit' and 'Surplus' of Prototype Future Occupation Profiles (FOP) against existing training provision e.g. Institute for Apprenticeships and Technical Education (IfATE).* *It is possible for the 'Fit' and 'Surplus' comparison to total over 100%, as they are two separate calculations based on a two-way comparison.*
Fit & Surplus Matrix	*This page is a visual representation of the 'Fit and Surplus Factor' insight. You can visually review 'Fit' and 'Surplus' of Prototype Future Occupation Profiles (FOP) against existing training provision e.g. Institute for Apprenticeships and Technical Education (IfATE).* *This can help you identify which provision may align strongest, or which may require adaptation, to provide the suitable provision fit for each future role.* *It will help you focus in on which provision to focus your attention for analysis.*
FOP Capability Matches	*This page allows you to view the matches between Capabilities and Institute for Apprenticeships and Technical Education (IfATE) Duty Statements. Clicking the arrow next to a number in the 'Matches' column will open a popup with more detail for each Capability.* *Each capability also includes Knowledge, Skill and Behaviour Tags, to support with scaffolding future education provision.* *You can review individual Prototype Future Occupational Profiles (FOPs) or review all FOPs under a Role Level, to give a more holistic view of Capabilities and Matches* *Where a future capability has been matched to existing provision (currently, by default, IfATE apprenticeship standards) it is possible to interrogate the data and identify specific statements in standards that align to enable identification of existing training materials and activities that could be used or adapted to meet future requirements.* *This can be used to review the capability requirements for Role Levels and FOPs, from Job / Occupation level through to Knowledge, Skill and Behaviour level*

4. Conclusion and Next Steps

4. Conclusions and Next Steps

4.1 Summary of Key Insights

The below table counts the number of IfATE standards[7] by suitability score for each FOP. For the purpose of this report, we've utilised the suitability grid to highlight the top IfATE standards that support each FOP. The table identifies if they have low, some or high suitability and colour-coded their overall suitability.

Role Level	Primary Supply Chain / Supply Chain Partner	Future Occupation Profile	Low Suitability	Some Suitability	High Suitability	Overall Suitability RAG
Senior Level	Research and Development Organisations	Research Scientist (Simulation)	9	1	0	Some
Senior Level	National Cyber Security Centre, Regulators and Auditors	Compliance Officer (Simulation)	10	0	0	Low
Senior Level	National Cyber Security Centre, Regulators and Auditors	Cybersecurity Auditor	10	0	0	Low
Senior Level	National Cyber Security Centre, Regulators and Auditors	Senior Digital Twin Specialist	10	0	0	Low
Senior Level	Research and Development Organisations, Transport Operators	Cybersecurity Innovation Lead	10	0	0	Low
Mid-Level	Software Development Companies / Suppliers	BIM Specialist	10	0	0	Low
Mid-Level	Software Development Companies / Suppliers	Cybersecurity Specialist	9	1	0	Some
Mid-Level	Software Development Companies / Suppliers	Software Developer	10	0	0	Low
Mid-Level	Systems Integration Specialists Consultants	Cybersecurity Consultant	9	1	0	Some
Mid-Level	Systems Integration Specialists Consultants	Systems Integration Specialist	10	0	0	Low

[7] Apprenticeship standards show what an apprentice will be doing and the skills required of them, by job role. The full list of current apprenticeship standards is accessible following this link.

Mid-Level	National Cyber Security Centre	Simulation Engineer	10	0	0	Low
Mid-Level	National Cyber Security Centre, Regulators and Auditors	Digital Twin Specialist	10	0	0	Low
Mid-Level	Research and Development Organisations, Transport Operators	Prototyping Engineer	9	1	0	Some
Mid-Level	Research and Development Organisations, Transport Operators	Software Test Engineer	9	0	1	Good
Mid-Level	Software Development Companies / Suppliers, Systems Integration Specialists Consultants, Transport Operators	Project Manager	9	1	0	Some
Mid-Level	Transport Operators, National Cyber Security Centre	Compliance Officer	9	1	0	Some
Junior Level	Software Development Companies / Suppliers, Systems Integration Specialists Consultants	Digital Twin Engineer	10	0	0	Low
Junior Level	Software Development Companies / Suppliers, Transport Operators	Data Analyst	9	1	0	Some

Top Fits

By reviewing the FOPs against the suitability grid, we can determine which of the groups of current apprenticeship standards are more applicable than others.

The ‘IT solutions architects and designers’ FOP has 1 IfATE apprenticeship standard that has a high suitability level against the standard, whilst the rest of the IfATE apprenticeship standards have low scoring standards.

Suitable standards are listed in the table below:

Role Level	Future Occupation Profile	IfATE Apprenticeship Standard	Suitability
Mid-Level	Software Test Engineer	Cyber security technologist (2021)	Good
Mid-Level	Software Test Engineer	Digital and technology solutions professional	Good
Mid-Level	Software Test Engineer	Cyber security technical professional (integrated degree)	Good
Mid-Level	Software Test Engineer	Software tester	Good
Mid-Level	Software Test Engineer	High integrity software engineer	Good
Mid-Level	Software Test Engineer	Protective security adviser	Good
Mid-Level	Software Test Engineer	Intelligence analyst	Good
Mid-Level	Software Test Engineer	Transport planner (integrated degree)	Good
Mid-Level	Software Test Engineer	Process automation engineer (degree)	Good
Mid-Level	Software Test Engineer	Automation and controls engineering technician	Good

The use of the data visualisation tool is recommended to access the next layer of detail and review the specific standards that have been identified as having Good Suitability / Some Suitability or Low Suitability.

As a comparison we can also list the standards that score lowest against the required FOPs, suggesting that there are very little suitable in the IfATE standards to support these Future Role Profiles.

FOPs with the lowest scores are:

1. Compliance Officer (Simulation)
2. Cybersecurity Auditor
3. Senior Digital Twin Specialist
4. Cybersecurity Innovation Lead
5. BIM Specialist
6. Software Developer
7. Systems Integration Specialist
8. Simulation Engineer
9. Digital Twin Specialist
10. Digital Twin Engineer

Our analysis reveals that certain FOPs have emerged with notably low scores, suggesting that key areas of skills alignment may be underdeveloped. Ten roles, spanning Compliance, Auditing and Simulation, stand out for their limited fit within the current qualification frameworks. This misalignment is particularly evident in that only one of the FOPs that surfaced from this cycle strongly align with the IfATE standards, highlighting a disconnect between the emerging industry demands and the established educational criteria.

This gap implies that new roles might enter the market without formalised training pathways, necessitating targeted curriculum development or revisions in apprenticeship models. Similarly, roles focused on simulation and compliance call for specialised qualifications that are not yet adequately represented. Even within cybersecurity, positions such as Auditor may require updates to existing certification frameworks to address the rapidly evolving nature of digital threats and technologies.

4.2 What this means for Industry and the Workforce

The primary insight from this Cycle’s report is that, while it has delivered comprehensive intelligence on the essential changes needed within the supply chain, workforce, and education system, this represents just the first step in the larger Skills Value Chain. What is now required is collective action from all stakeholders.

This means adopting proactive strategies to ensure emerging skilled professionals are well-equipped to meet future demands for the industry, particularly in the transport and cybersecurity Sectors. Organisations must ensure that their employees are trained in threat simulation and security validation and proficient in managing the convergence of IT and OT. Building a robust future talent pipeline will require active collaboration with educational institutions, from schools to universities, and training providers, aligning education pathways with the industry’s requirements. Moreover, a cross-sector approach is essential; the lessons learned from workforce foresighting should inform practices in transport tunnels and extrapolate across other critical infrastructure domains.

As the sector evolves, organisational structures must be reassessed to understand the impact on workforce roles and cybersecurity operations. Establishing dedicated working groups and industry consortia can help shape digital twin-enabled cybersecurity solutions, ensuring that these capabilities are embedded at every stage of project development, from design through to operational implementation. Employers can mitigate the risk of talent shortages by anticipating future skill requirements and managing workforce transformations early.

Furthermore, closing the skills gap hinges on aligning workforce demand with targeted training and education initiatives. This will involve forging partnerships with educational institutions to create training programs focusing on cyber-physical security and digital twin applications and ensuring these initiatives align with standards set by bodies like IfATE and Innovate UK. Investments in specialist training centres that emphasise simulation-based learning and real-world threat modelling will also be essential. Through these coordinated actions, the sector can secure a workforce that is not only capable of managing digital twin-enabled cybersecurity operations but is also prepared to support the long-term resilience of transport infrastructure against emerging threats.

4.3 What this means for Education

The findings of the foresighting study indicate that the sector can meet future cybersecurity and digital twin technology workforce needs by making focused modifications to existing courses and degrees rather than overhauling them entirely. The FOPs and capability sets developed during the cycle reveal that a modular approach to curriculum development is sufficient and achievable within the necessary timescales. This approach allows educators to integrate essential skills without the disruption that a complete course redesign entails.

In the engineering context, while the study prominently featured computer science examples, there was also a considerable emphasis on electrical and mechanical engineering. This insight suggests that education modules for higher and further education should be designed to address occupational profiles and capability sets in electrical, mechanical, and systems integration engineering – with a particular emphasis on cross-training the workforce between these domains.

For those areas that require more specialised technical expertise, this cycle recommends leveraging routes such as PhD sponsorships and closer engagement with industry. University-led PhD research can provide a detailed examination of emerging problems and technologies, setting the stage for industry professionals and registered training organisations to refine and scale these solutions. Early identification of these specialist areas is necessary so academia can proactively engage with industry, enabling a collaborative dialogue that helps shape relevant research topics.

The implications for curriculum development are significant. Higher education and further education providers must adapt their courses to incorporate skills such as digital twin cybersecurity applications – including simulating cyber threats, risk modelling, and security validation – and addressing OT's convergence with IT. Moreover, the growing role of AI in threat detection and predictive analytics suggests that these areas should be introduced as specialist modules within existing cybersecurity, computer science, and engineering programmes.

The foresighting cycle further highlights that while digital twin applications are primarily associated with BIM and infrastructure management, they also have strong links to transport infrastructure, cyber-physical security, and data analytics. As such, cybersecurity programmes must include modules on digital twin risk assessment and cyber-physical security simulation, engineering disciplines integrate digital twin modelling for system performance validation and predictive maintenance, and transport infrastructure management courses incorporate cyber-resilience training to address digital threats. Cross-disciplinary training will expose students to technical cybersecurity principles and the challenges of managing digitised infrastructure, from both the perspectives of OT and IT.

Our findings suggest that addressing highly specialised areas such as digital twin security, advanced cyber-physical risk modelling, and regulatory compliance for transport cybersecurity requires a multi-disciplinary approach. Universities and research centres should consider developing PhD sponsorships and industry research partnerships. Such initiatives allow academic investigations to tackle cutting-edge challenges in collaboration with businesses, ensuring that research remains relevant and impactful.

Alongside these academic routes, there is a clear need for industry-led continuing professional development programmes. These programmes provide cybersecurity professionals with upskilling pathways that reflect the rapidly evolving nature of the field. When gaps in capability persist, close collaboration among universities, technical colleges, and employers becomes essential to ensure that training programmes remain closely aligned with the practical demands of the job market.

We recognise and appreciate the challenge for academic institutions to engage proactively with industry. Regular dialogue between industry and academia can help ensure curriculum development responds to emerging technological needs. Universities are encouraged to offer flexible, modular training programmes that embed digital twin cybersecurity skills into both undergraduate and postgraduate education, thereby equipping students with the practical expertise needed for modern challenges. Further education providers should also work closely with industry to develop apprenticeship pathways, which will help new entrants acquire the digital skills necessary to thrive in this dynamic environment.

4.4 Recommended next steps

The recommended next steps call for a clear, collective effort to prepare the transport sector for the growing demands of digital twin cybersecurity. The approach is to update existing courses using FOPs to pinpoint skill gaps rather than overhauling programs entirely. A dedicated working group should be formed with industry players, educators, and government bodies to drive the integration of digital twin security training. This group will validate future roles by engaging with employers and mapping skills needs against current training.

In the short term (2027-2028), pilot projects should introduce digital twin cybersecurity modules, aligning apprenticeships and degree pathways with immediate needs. These efforts should be scaled across the sector over the mid-term (2028-2032) and embedded into regulatory frameworks.

Failing to act risks leaving critical infrastructure vulnerable, widening the skills gap, and reducing the UK's global competitiveness. Coordinated action now will help secure a workforce ready to manage digital twin cybersecurity challenges and strengthen national security.

- **Refine Skill Gap Identification**
  - Use Foresight-Optimised Pathways (FOPs) to pinpoint cybersecurity skill gaps in digital twin applications
  - Update existing courses based on findings rather than undertaking a full curriculum overhaul
- **Establish a Digital Twin Cybersecurity Working Group**
  - Form a coalition of industry leaders, educators, and government bodies
  - Define clear objectives for integrating digital twin security training
- **Validate Future Roles and Training Needs**
  - Engage directly with employers to define critical cybersecurity roles
  - Map skill requirements against current training programs to highlight gaps
- **Launch Pilot Training Modules (2027-2028)**
  - Develop and test digital twin cybersecurity modules in apprenticeships and degree programs
  - Align new training elements with emerging industry needs
- **Scale and Standardise Training (2028-2032)**

- Expand successful pilot projects across the transport sector
  - Integrate digital twin security training into regulatory frameworks to ensure long-term adoption
- **Drive Urgent, Coordinated Action**
  - Prevent critical infrastructure vulnerabilities by addressing workforce shortages now
  - Position the UK as a global leader in digital twin cybersecurity readiness

5. Appendix

5. Appendices

Section	Title
5.1	List of participants
5.2	Cycle timeline
5.3	Access to output data - link and authorisation
5.4	Glossary - common language
5.5	Visualisation links and illustrations

5.1 List of Participants

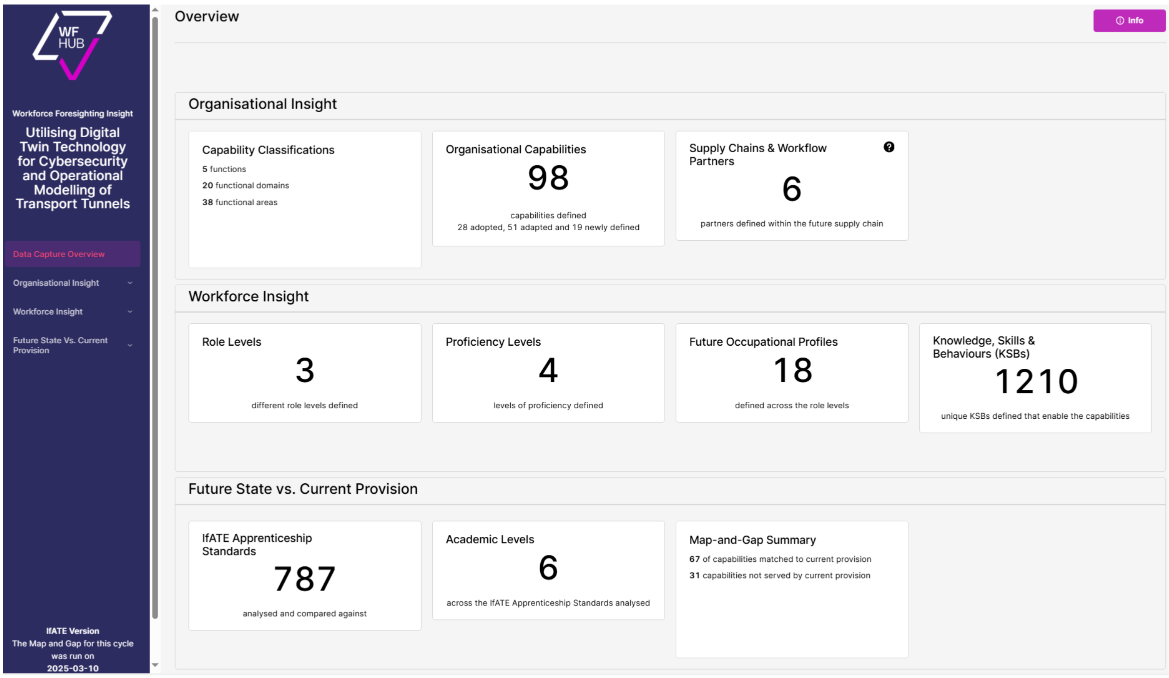
Employers	Educators	Technologists
Keith Price – National Highways	Abdullahi Arabo - University of the West of England	Tim Parker – PA Consulting
Oliver Lacey – National Highways	Navid Abapour – University of Surrey	Xicheng Li – University of Glasgow
Stephen Luke – National Highways		Minesh Vaghjiani – Department for Transport
Mark McAleer – BDO		Pavlos Padadopoulos – Edinburgh Napier University
Andrew MacLachlan – Cyber Warden		
Lizzy Morgan – Civil Aviation Authority		
Luke Martin-Farla - AtkinsRéalis		

5.2 Cycle timeline

Workforce Foresighting cycle started the Carry Out phase in November 2024. The Carry Out phase concluded in February 2025. The Findings report was prepared following the data validation period and published in March 2025.

5.3 Access to output data - link and authorisation

Link to Visualisation Tool



Workforce Foresighting Insight

Utilising Digital Twin Technology for Cybersecurity and Operational Modelling of Transport Tunnels

Data Capture Overview

Organisational Insight

Workforce Insight

Future State Vs. Current Provision

IfATE Version
The Map and Gap for this cycle was run on
2025-03-10

Overview

Info

Organisational Insight

Capability Classifications
5 functions
20 functional domains
38 functional areas

Organisational Capabilities
98
capabilities defined
28 adopted, 51 adapted and 19 newly defined

Supply Chains & Workflow Partners
6
partners defined within the future supply chain

Workforce Insight

Role Levels
3
different role levels defined

Proficiency Levels
4
levels of proficiency defined

Future Occupational Profiles
18
defined across the role levels

Knowledge, Skills & Behaviours (KSBs)
1210
unique KSBs defined that enable the capabilities

Future State vs. Current Provision

IfATE Apprenticeship Standards
787
analysed and compared against

Academic Levels
6
across the IfATE Apprenticeship Standards analysed

Map-and-Gap Summary
67 of capabilities matched to current provision
31 capabilities not served by current provision

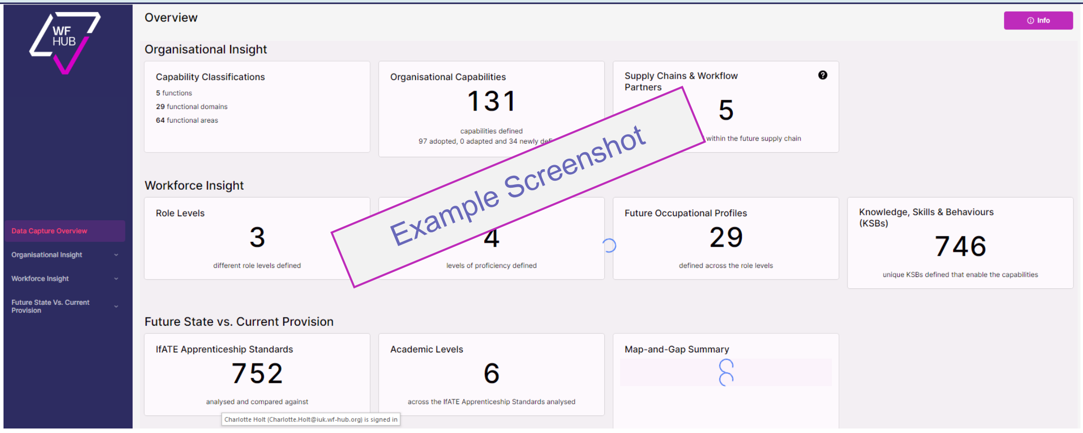
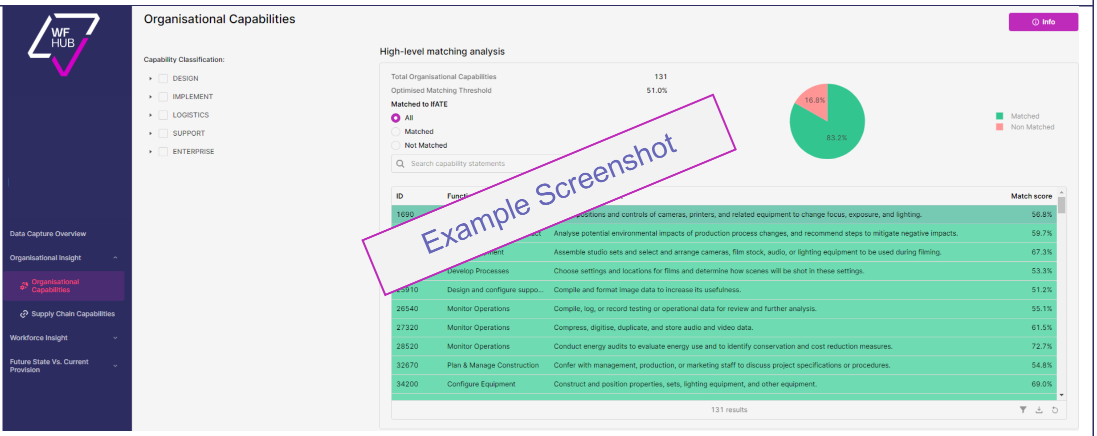
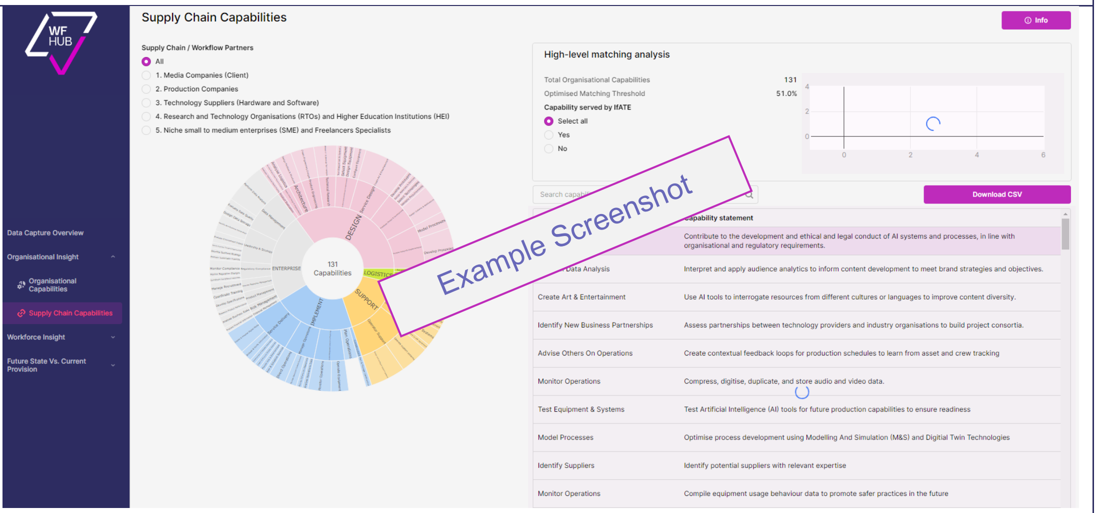
5.4 Glossary - common language

Term	Definition
Impact Domains	Innovate UK domains used as Strategic Categories to assist setting and monitoring priorities
National Challenge (Industry / Sector / Region)	A recognised technological or socio-political threat or opportunity for which there is consensus that workforce action is necessary
Challenge Response	Specific intervention aimed at the challenge
Capability (Organisation)	The collective abilities, and expertise of an organisation to carry out a function, because provision and preparation have been made by the organisation
Capability Classification	Classification provides a common, structured vocabulary to define capability
Capability Statements	Description of the depth and nature of each capability within an organisation
Capability Syntax	Common language to describe each capability application within organisation type
Competencies (Workforce / Individual)	'Proficiency, aptitude, capacity, skill, technique, experience, expertise, facility, fitness related to capability
Competency definition 'KSBs' (Knowledge, Skills and Behaviours)	Knowledge, Skills, and Behaviours are the elements used to express the required competencies for each Role Group
Competency Domain	Used during foresighting analysis to provide focus on existing and emerging competency needs
Delphi Process	Foresighting takes a Delphi approach which has come to represent consulting expert opinion. (Harking back to the Delphic Oracle of ancient Greece)
Foresight Cycle	Set of workshops, analysis and reporting that implements the Foresight Process for each subject
Foresight Process	A series of activities which are convened to understand future competence needs, the opportunities available and actions required to deliver the right skills at the right time and place

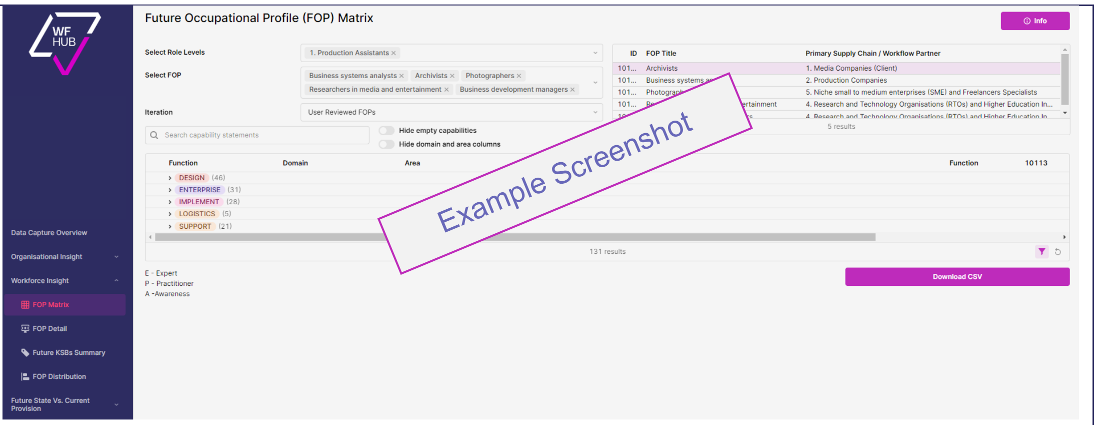
Foresighting Champion	An individual nominated within a new user organisation of foresighting to facilitate and lead the use of foresighting processes and tools with the support of the Project Team
Foresighting Subject	The application of specific technologies in the context of a given challenge and which are candidates for foresighting
Future Competency Set	The KBS output from the Educator workshop for each Role Group
Map and Gap Analysis	A combined expert and automated process that maps the Future Competency Set against a selected reference framework
Organisation Type	Simple description of nature of organisation for which capability is required
Proficiencies	Proficiencies differentiate the degree of competencies required from differing Role Groups to support capabilities
Project Sponsor	Typically, a stakeholder in the challenge being successfully met who requires information to under-write plans to act
Role Group	Role groups are a collective of roles that exist in a typical manufacturing business / industrial sector
Syntax	The way in which a statement is phrased to ensure reliable, repeatable and meaningful interpretation
Technologies	The technology that could be used to address the challenge
Working Scenario	To provide further context in relation to the subjects and used to position participants thinking during the detailed identification of future capabilities
Workshops	Online sessions used to undertake each step in the foresight process
Roadmaps	Sector, Industry, Regional view of emerging opportunities and their market entry
Participants	Technologists, Educators, Employers

5.5 – Visualisation links and Illustrations

Images are not cycle specific and just for guidance purposes

Link to Visualisation	View of data
Data Capture Overview	 Overview ⓘ Info Organisational Insight Capability Classifications: 5 functions, 29 functional domains, 64 functional areas Organisational Capabilities: 131 capabilities defined, 97 adopted, 0 adapted and 34 newly def Supply Chains & Workflow Partners: 5 within the future supply chain Workforce Insight Role Levels: 3 different role levels defined 4 levels of proficiency defined Future Occupational Profiles: 29 defined across the role levels Knowledge, Skills & Behaviours (KSBs): 746 unique KSBs defined that enable the capabilities Future State vs. Current Provision IfATE Apprenticeship Standards: 752 analysed and compared against Academic Levels: 6 across the IfATE Apprenticeship Standards analysed Map-and-Gap Summary Charlotte Holt (Charlotte.Holt@iuk.wf-hub.org) is signed in WF HUB Data Capture Overview Organisational Insight Workforce Insight Future State Vs. Current Provision Example Screenshot
Organisational Capabilities	 Organisational Capabilities ⓘ Info Capability Classification: □ DESIGN, □ IMPLEMENT, □ LOGISTICS, □ SUPPORT, □ ENTERPRISE High-level matching analysis Total Organisational Capabilities 131 Optimised Matching Threshold 51.0% Matched to IfATE: ● All ○ Matched ○ Not Matched Search capability statements ID / Functi… / Match score 1690 … positions and controls of cameras, printers, and related equipment to change focus, exposure, and lighting. 56.8% …ct Analyse potential environmental impacts of production process changes, and recommend steps to mitigate negative impacts. 59.7% …ment Assemble studio sets and select and arrange cameras, film stock, audio, or lighting equipment to be used during filming. 67.3% Develop Processes Choose settings and locations for films and determine how scenes will be shot in these settings. 53.3% 25910 Design and configure suppo… Compile and format image data to increase its usefulness. 51.2% 26540 Monitor Operations Compile, log, or record testing or operational data for review and further analysis. 55.1% 27320 Monitor Operations Compress, digitise, duplicate, and store audio and video data. 61.5% 28520 Monitor Operations Conduct energy audits to evaluate energy use and to identify conservation and cost reduction measures. 72.7% 32670 Plan & Manage Construction Confer with management, production, or marketing staff to discuss project specifications or procedures. 54.8% 34200 Configure Equipment Construct and position properties, sets, lighting equipment, and other equipment. 69.0% 131 results WF HUB 16.8% 83.2% 🟩 Matched 🟥 Non Matched Data Capture Overview Organisational Insight Organisational Capabilities Supply Chain Capabilities Workforce Insight Future State Vs. Current Provision Example Screenshot
Supply Chain Capabilities	 Supply Chain Capabilities ⓘ Info Supply Chain / Workflow Partners ● All ○ 1. Media Companies (Client) ○ 2. Production Companies ○ 3. Technology Suppliers (Hardware and Software) ○ 4. Research and Technology Organisations (RTOs) and Higher Education Institutions (HEI) ○ 5. Niche small to medium enterprises (SME) and Freelancers Specialists High-level matching analysis Total Organisational Capabilities 131 Optimised Matching Threshold 51.0% Capability served by IfATE: ● Select all ○ Yes ○ No Search capab… Download CSV …apability statement Contribute to the development and ethical and legal conduct of AI systems and processes, in line with organisational and regulatory requirements. … Data Analysis Interpret and apply audience analytics to inform content development to meet brand strategies and objectives. Create Art & Entertainment Use AI tools to interrogate resources from different cultures or languages to improve content diversity. Identify New Business Partnerships Assess partnerships between technology providers and industry organisations to build project consortia. Advise Others On Operations Create contextual feedback loops for production schedules to learn from asset and crew tracking Monitor Operations Compress, digitise, duplicate, and store audio and video data. Test Equipment & Systems Test Artificial Intelligence (AI) tools for future production capabilities to ensure readiness Model Processes Optimise process development using Modelling And Simulation (M&S) and Digitial Twin Technologies Identify Suppliers Identify potential suppliers with relevant expertise Monitor Operations Compile equipment usage behaviour data to promote safer practices in the future WF HUB 131 Capabilities DESIGN IMPLEMENT SUPPORT LOGISTICS ENTERPRISE Architecture Service Design Service Delivery 4 2 0 0 2 4 6 Data Capture Overview Organisational Insight Organisational Capabilities Supply Chain Capabilities Workforce Insight Future State Vs. Current Provision Example Screenshot

FOP Matrix



Future Occupational Profile (FOP) Matrix

Select Role Levels: 1. Production Assistants ×

Select FOP: Business systems analysts × Archivists × Photographers × Researchers in media and entertainment × Business development managers ×

Iteration: User Reviewed FOPs

Search capability statements

Hide empty capabilities

Hide domain and area columns

ID	FOP Title	Primary Supply Chain / Workflow Partner
101...	Archivists	1. Media Companies (Client)
101...	Business systems a	2. Production Companies
101...	Photograph	5. Niche small to medium enterprises (SME) and Freelancers Specialists
101...	Re ertainment	4. Research and Technology Organisations (RTOs) and Higher Education In...
10	rs	4. Research and Technology Organisations (RTOs) and Higher Education In...

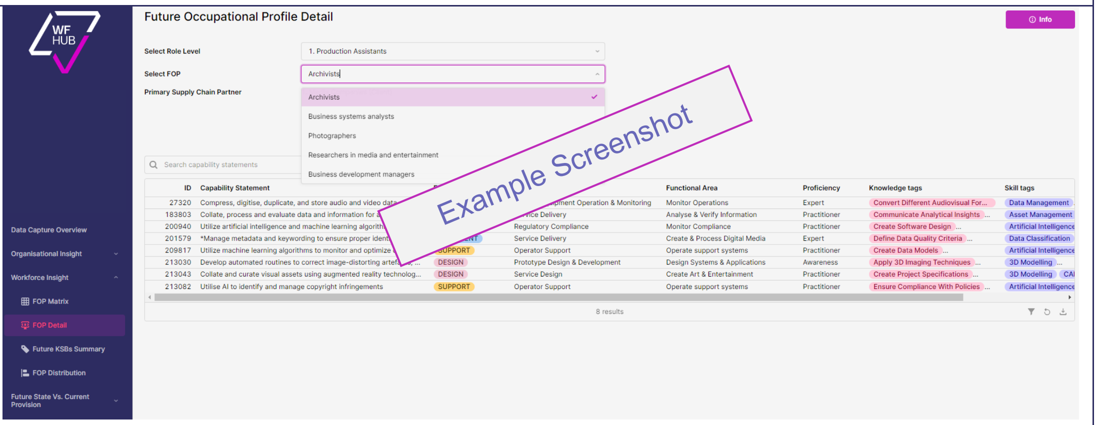
5 results

Function	Domain	Area	Function	10113
› DESIGN (46)				
› ENTERPRISE (31)				
› IMPLEMENT (28)				
› LOGISTICS (5)				
› SUPPORT (21)				

131 results

E - Expert
P - Practitioner
A -Awareness

FOP Detail



Future Occupational Profile Detail

Select Role Level: 1. Production Assistants

Select FOP: Archivists

Primary Supply Chain Partner

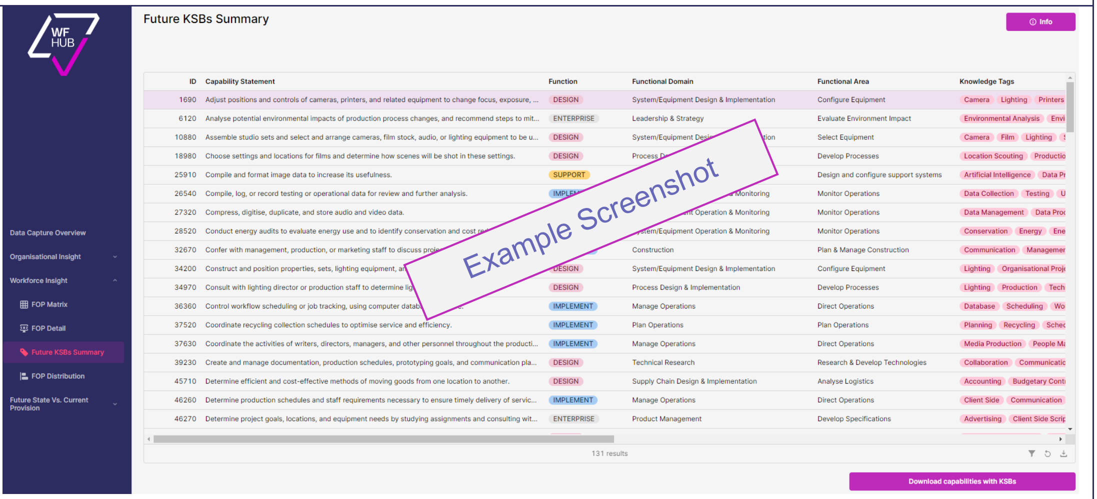
- Archivists ✓
- Business systems analysts
- Photographers
- Researchers in media and entertainment
- Business development managers

Search capability statements

ID	Capability Statement			Functional Area	Proficiency	Knowledge tags	Skill tags
27320	Compress, digitise, duplicate, and store audio and video data		pment Operation & Monitoring	Monitor Operations	Expert	Convert Different Audiovisual For...	Data Management
183803	Collate, process and evaluate data and information for a		vice Delivery	Analyse & Verify Information	Practitioner	Communicate Analytical Insights ...	Asset Management
200940	Utilize artificial intelligence and machine learning algorith		Regulatory Compliance	Monitor Compliance	Practitioner	Create Software Design ...	Artificial Intelligence
201579	*Manage metadata and keywording to ensure proper ident	ENT	Service Delivery	Create & Process Digital Media	Expert	Define Data Quality Criteria ...	Data Classification
209817	Utilize machine learning algorithms to monitor and optimize	SUPPORT	Operator Support	Operate support systems	Practitioner	Create Data Models ...	Artificial Intelligence
213030	Develop automated routines to correct image-distorting artef , ...	DESIGN	Prototype Design & Development	Design Systems & Applications	Awareness	Apply 3D Imaging Techniques ...	3D Modelling ...
213043	Collate and curate visual assets using augmented reality technolog...	DESIGN	Service Design	Create Art & Entertainment	Practitioner	Create Project Specifications ...	3D Modelling CAI
213082	Utilise AI to identify and manage copyright infringements	SUPPORT	Operator Support	Operate support systems	Practitioner	Ensure Compliance With Policies ...	Artificial Intelligence

8 results

Future KSBs Summary

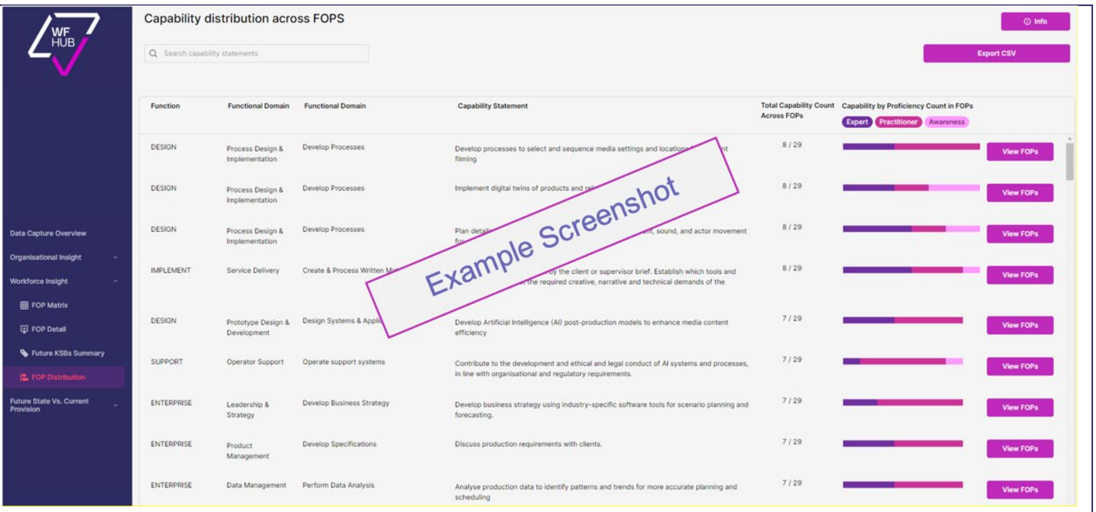


Future KSBs Summary

ID	Capability Statement	Function	Functional Domain	Functional Area	Knowledge Tags
1690	Adjust positions and controls of cameras, printers, and related equipment to change focus, exposure, ...	DESIGN	System/Equipment Design & Implementation	Configure Equipment	Camera Lighting Printers
6120	Analyse potential environmental impacts of production process changes, and recommend steps to mit...	ENTERPRISE	Leadership & Strategy	Evaluate Environment Impact	Environmental Analysis Envi
10880	Assemble studio sets and select and arrange cameras, film stock, audio, or lighting equipment to be u...	DESIGN	System/Equipment Desi tion	Select Equipment	Camera Film Lighting
18980	Choose settings and locations for films and determine how scenes will be shot in these settings.	DESIGN	Process D	Develop Processes	Location Scouting Productio
25910	Compile and format image data to increase its usefulness.	SUPPORT		Design and configure support systems	Artificial Intelligence Data Pr
26540	Compile, log, or record testing or operational data for review and further analysis.	IMPLE	Monitoring	Monitor Operations	Data Collection Testing U
27320	Compress, digitise, duplicate, and store audio and video data.		nt Operation & Monitoring	Monitor Operations	Data Management Data Proc
28520	Conduct energy audits to evaluate energy use and to identify conservation and cost re		stem/Equipment Operation & Monitoring	Monitor Operations	Conservation Energy Ene
32670	Confer with management, production, or marketing staff to discuss proje		Construction	Plan & Manage Construction	Communication Managemer
34200	Construct and position properties, sets, lighting equipment, ar	DESIGN	System/Equipment Design & Implementation	Configure Equipment	Lighting Organisational Proje
34970	Consult with lighting director or production staff to determine lig	DESIGN	Process Design & Implementation	Develop Processes	Lighting Production Tech
36360	Control workflow scheduling or job tracking, using computer datab e.	IMPLEMENT	Manage Operations	Direct Operations	Database Scheduling Wo
37520	Coordinate recycling collection schedules to optimise service and efficiency.	IMPLEMENT	Plan Operations	Plan Operations	Planning Recycling Schec
37630	Coordinate the activities of writers, directors, managers, and other personnel throughout the producti...	IMPLEMENT	Manage Operations	Direct Operations	Media Production People Ma
39230	Create and manage documentation, production schedules, prototyping goals, and communication pla...	DESIGN	Technical Research	Research & Develop Technologies	Collaboration Communicatic
45710	Determine efficient and cost-effective methods of moving goods from one location to another.	DESIGN	Supply Chain Design & Implementation	Analyse Logistics	Accounting Budgetary Conti
46260	Determine production schedules and staff requirements necessary to ensure timely delivery of servic...	IMPLEMENT	Manage Operations	Direct Operations	Client Side Communication
46270	Determine project goals, locations, and equipment needs by studying assignments and consulting wit...	ENTERPRISE	Product Management	Develop Specifications	Advertising Client Side Scrip

131 results

FOP Distribution



Data Capture Overview
Organisational Insight
Workforce Insight
FOP Matrix
FOP Detail
Future KSBs Summary
FOP Distribution
Future State Vs. Current Provision

Capability distribution across FOPS

ⓘ Info

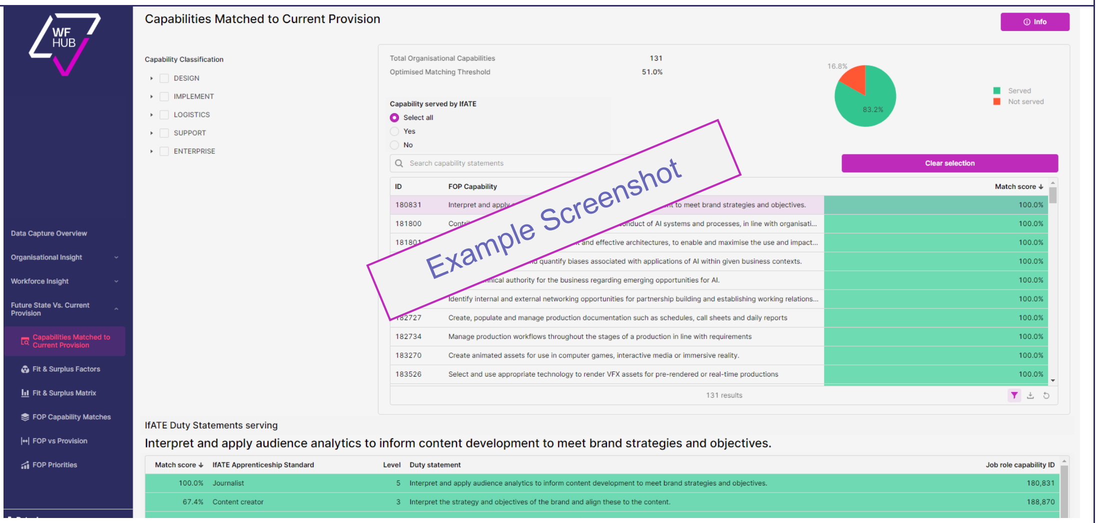
Search capability statements

Export CSV

Function	Functional Domain	Functional Domain	Capability Statement	Total Capability Count Across FOPs	Capability by Proficiency Count in FOPs Expert Practitioner Awareness	
DESIGN	Process Design & Implementation	Develop Processes	Develop processes to select and sequence media settings and locations nt filming	8 / 29		View FOPs
DESIGN	Process Design & Implementation	Develop Processes	Implement digital twins of products and re	8 / 29		View FOPs
DESIGN	Process Design & Implementation	Develop Processes	Plan detai fo nt, sound, and actor movement	8 / 29		View FOPs
IMPLEMENT	Service Delivery	Create & Process Written M	by the client or supervisor brief. Establish which tools and the required creative, narrative and technical demands of the	8 / 29		View FOPs
DESIGN	Prototype Design & Development	Design Systems & Appli	Develop Artificial Intelligence (AI) post-production models to enhance media content efficiency	7 / 29		View FOPs
SUPPORT	Operator Support	Operate support systems	Contribute to the development and ethical and legal conduct of AI systems and processes, in line with organisational and regulatory requirements.	7 / 29		View FOPs
ENTERPRISE	Leadership & Strategy	Develop Business Strategy	Develop business strategy using industry-specific software tools for scenario planning and forecasting.	7 / 29		View FOPs
ENTERPRISE	Product Management	Develop Specifications	Discuss production requirements with clients.	7 / 29		View FOPs
ENTERPRISE	Data Management	Perform Data Analysis	Analyse production data to identify patterns and trends for more accurate planning and scheduling	7 / 29		View FOPs

Example Screenshot

Capabilities Matched to Current Provision



Data Capture Overview
Organisational Insight
Workforce Insight
Future State Vs. Current Provision
Capabilities Matched to Current Provision
Fit & Surplus Factors
Fit & Surplus Matrix
FOP Capability Matches
FOP vs Provision
FOP Priorities

Capabilities Matched to Current Provision

ⓘ Info

Capability Classification
- □ DESIGN
- □ IMPLEMENT
- □ LOGISTICS
- □ SUPPORT
- □ ENTERPRISE

Total Organisational Capabilities 131
Optimised Matching Threshold 51.0%

Capability served by IfATE
- ● Select all
- ○ Yes
- ○ No

Search capability statements

Clear selection

ID	FOP Capability	Match score ↓
180831	Interpret and apply nt to meet brand strategies and objectives.	100.0%
181800	Contr onduct of AI systems and processes, in line with organisati...	100.0%
181801	and effective architectures, to enable and maximise the use and impact...	100.0%
	d quantify biases associated with applications of AI within given business contexts.	100.0%
	nical authority for the business regarding emerging opportunities for AI.	100.0%
	Identify internal and external networking opportunities for partnership building and establishing working relations...	100.0%
82727	Create, populate and manage production documentation such as schedules, call sheets and daily reports	100.0%
182734	Manage production workflows throughout the stages of a production in line with requirements	100.0%
183270	Create animated assets for use in computer games, interactive media or immersive reality.	100.0%
183526	Select and use appropriate technology to render VFX assets for pre-rendered or real-time productions	100.0%

131 results

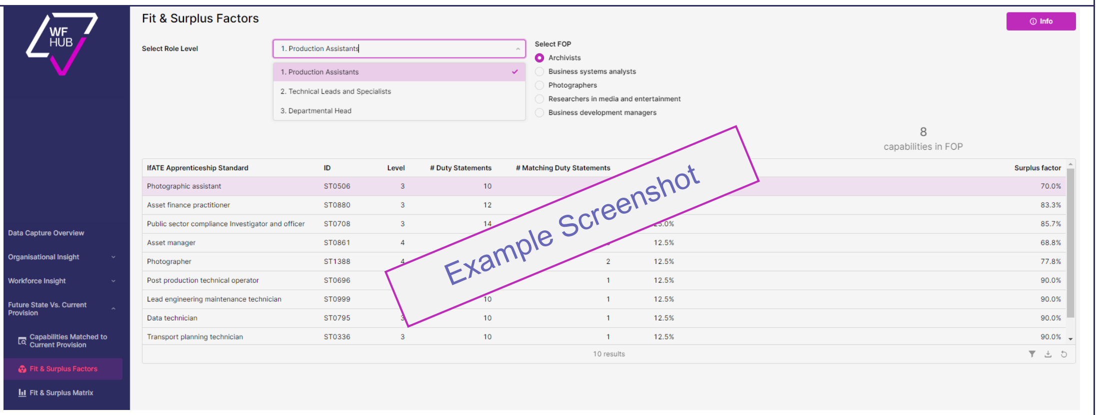
IfATE Duty Statements serving

Interpret and apply audience analytics to inform content development to meet brand strategies and objectives.

Match score ↓	IfATE Apprenticeship Standard	Level	Duty statement	Job role capability ID
100.0%	Journalist	5	Interpret and apply audience analytics to inform content development to meet brand strategies and objectives.	180,831
67.4%	Content creator	3	Interpret the strategy and objectives of the brand and align these to the content.	188,870

Example Screenshot

Fit & Surplus Factors



Data Capture Overview
Organisational Insight
Workforce Insight
Future State Vs. Current Provision
Capabilities Matched to Current Provision
Fit & Surplus Factors
Fit & Surplus Matrix

Fit & Surplus Factors

ⓘ Info

Select Role Level: 1. Production Assistants
- 1. Production Assistants ✓
- 2. Technical Leads and Specialists
- 3. Departmental Head

Select FOP
- ● Archivists
- ○ Business systems analysts
- ○ Photographers
- ○ Researchers in media and entertainment
- ○ Business development managers

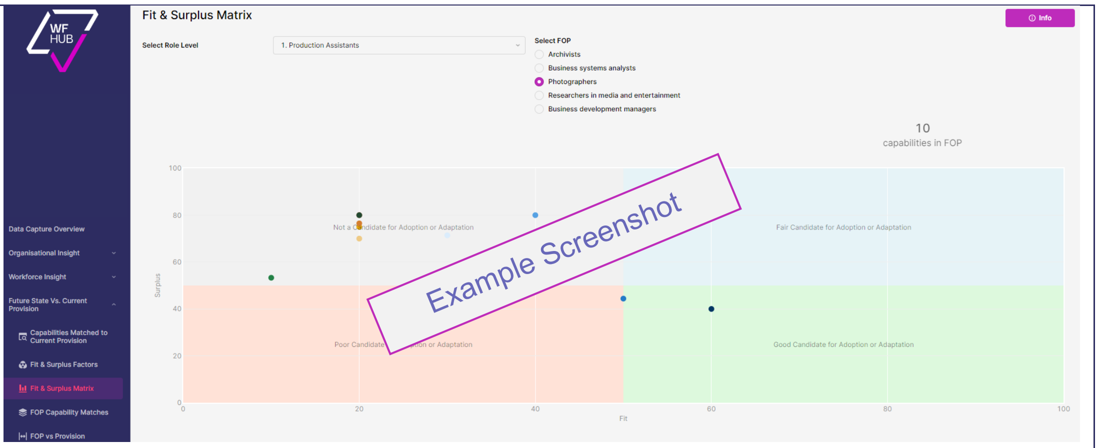
8
capabilities in FOP

IfATE Apprenticeship Standard	ID	Level	# Duty Statements	# Matching Duty Statements		Surplus factor
Photographic assistant	ST0506	3	10			70.0%
Asset finance practitioner	ST0880	3	12			83.3%
Public sector compliance Investigator and officer	ST0708	3	14		25.0%	85.7%
Asset manager	ST0861	4			12.5%	68.8%
Photographer	ST1388	4		2	12.5%	77.8%
Post production technical operator	ST0696			1	12.5%	90.0%
Lead engineering maintenance technician	ST0999		10	1	12.5%	90.0%
Data technician	ST0795	3	10	1	12.5%	90.0%
Transport planning technician	ST0336	3	10	1	12.5%	90.0%

10 results

Example Screenshot

Fit & Surplus Matrix


WF HUB
Data Capture Overview
Organisational Insight
Workforce Insight
Future State Vs. Current Provision
Capabilities Matched to Current Provision
Fit & Surplus Factors
Fit & Surplus Matrix
FOP Capability Matches
FOP vs Provision
Info
100
80
60
40
20
0
Surplus
0
20
40
60
80
100
Fit
Not a Candidate for Adoption or Adaptation
Fair Candidate for Adoption or Adaptation
Poor Candidate for Adoption or Adaptation
Good Candidate for Adoption or Adaptation
Example Screenshot

Fit & Surplus Matrix

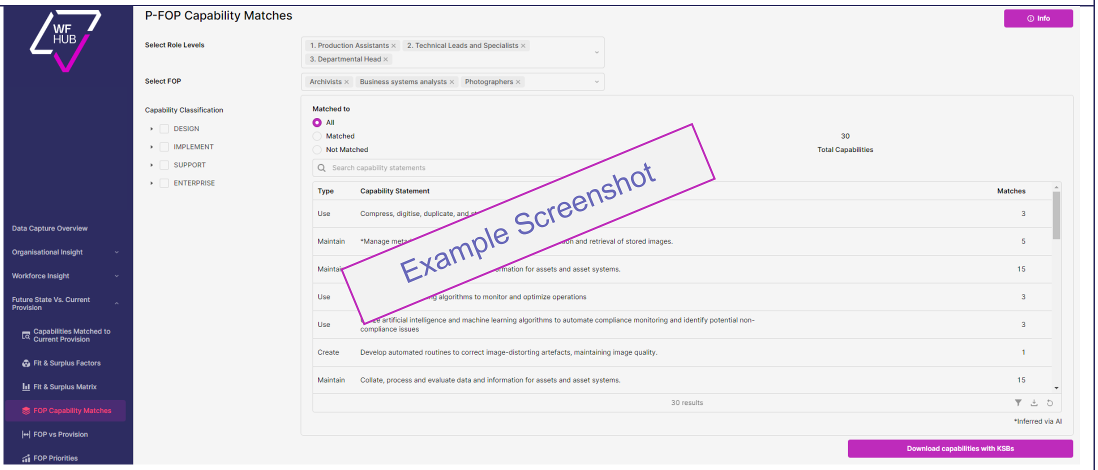
Select Role Level: 1. Production Assistants

Select FOP

- ○ Archivists
- ○ Business systems analysts
- ● Photographers
- ○ Researchers in media and entertainment
- ○ Business development managers

10
capabilities in FOP

FOP Capability Matches



P-FOP Capability Matches

Select Role Levels: 1. Production Assistants × 2. Technical Leads and Specialists × 3. Departmental Head ×

Select FOP: Archivists × Business systems analysts × Photographers ×

Capability Classification

- □ DESIGN
- □ IMPLEMENT
- □ SUPPORT
- □ ENTERPRISE

Matched to

- ● All
- ○ Matched
- ○ Not Matched

30
Total Capabilities

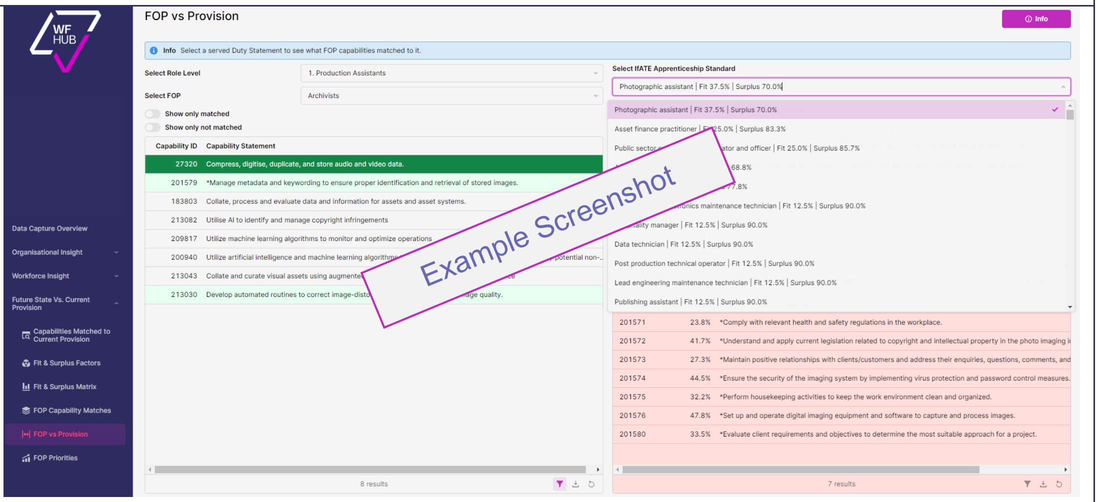
Search capability statements

Type	Capability Statement	Matches
Use	Compress, digitise, duplicate, and s	3
Maintain	*Manage met on and retrieval of stored images.	5
Maintai	rmation for assets and asset systems.	15
Use	g algorithms to monitor and optimize operations	3
Use	ze artificial intelligence and machine learning algorithms to automate compliance monitoring and identify potential non-compliance issues	3
Create	Develop automated routines to correct image-distorting artefacts, maintaining image quality.	1
Maintain	Collate, process and evaluate data and information for assets and asset systems.	15

30 results

*Inferred via AI

FOP vs Provision



FOP vs Provision

Info Select a served Duty Statement to see what FOP capabilities matched to it.

Select Role Level: 1. Production Assistants

Select FOP: Archivists

○ Show only matched

○ Show only not matched

Capability ID	Capability Statement
27320	Compress, digitise, duplicate, and store audio and video data.
201579	*Manage metadata and keywording to ensure proper identification and retrieval of stored images.
183803	Collate, process and evaluate data and information for assets and asset systems.
213082	Utilise AI to identify and manage copyright infringements
209817	Utilize machine learning algorithms to monitor and optimize operations
200940	Utilize artificial intelligence and machine learning algorithms potential non-..
213043	Collate and curate visual assets using augmente ce
213030	Develop automated routines to correct image-disto age quality.

8 results

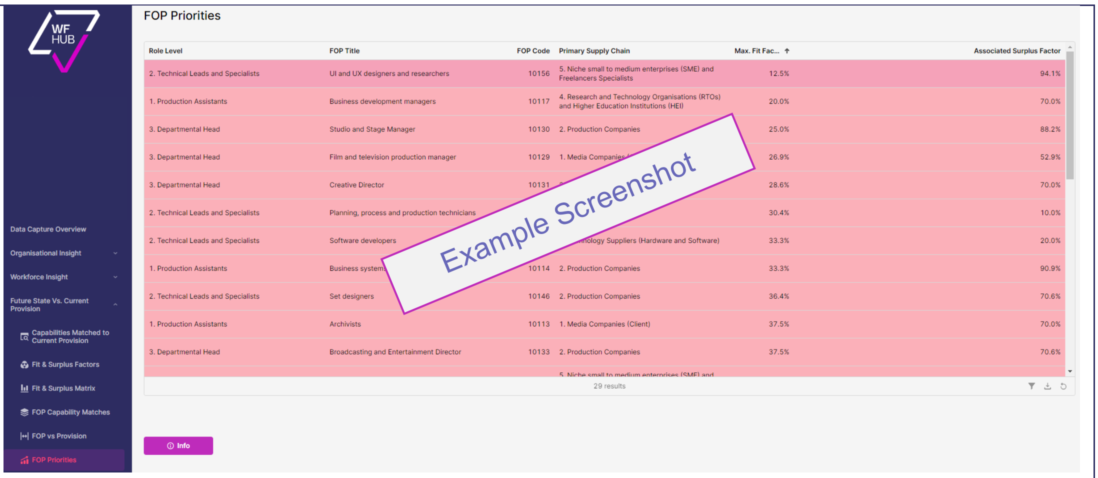
Select IfATE Apprenticeship Standard: Photographic assistant | Fit 37.5% | Surplus 70.0%

- Photographic assistant | Fit 37.5% | Surplus 70.0% ✓
- Asset finance practitioner | F 25.0% | Surplus 83.3%
- Public sector ator and officer | Fit 25.0% | Surplus 85.7%
- 68.8%
- 77.8%
- tronics maintenance technician | Fit 12.5% | Surplus 90.0%
- ality manager | Fit 12.5% | Surplus 90.0%
- Data technician | Fit 12.5% | Surplus 90.0%
- Post production technical operator | Fit 12.5% | Surplus 90.0%
- Lead engineering maintenance technician | Fit 12.5% | Surplus 90.0%
- Publishing assistant | Fit 12.5% | Surplus 90.0%

201571	23.8%	*Comply with relevant health and safety regulations in the workplace.
201572	41.7%	*Understand and apply current legislation related to copyright and intellectual property in the photo imaging i
201573	27.3%	*Maintain positive relationships with clients/customers and address their enquiries, questions, comments, and
201574	44.5%	*Ensure the security of the imaging system by implementing virus protection and password control measures.
201575	32.2%	*Perform housekeeping activities to keep the work environment clean and organized.
201576	47.8%	*Set up and operate digital imaging equipment and software to capture and process images.
201580	33.5%	*Evaluate client requirements and objectives to determine the most suitable approach for a project.

7 results

FOP Priorities



FOP Priorities

Role Level	FOP Title	FOP Code	Primary Supply Chain	Max. Fit Fac... ↑	Associated Surplus Factor
2. Technical Leads and Specialists	UI and UX designers and researchers	10156	5. Niche small to medium enterprises (SME) and Freelancers Specialists	12.5%	94.1%
1. Production Assistants	Business development managers	10117	4. Research and Technology Organisations (RTOs) and Higher Education Institutions (HEI)	20.0%	70.0%
3. Departmental Head	Studio and Stage Manager	10130	2. Production Companies	25.0%	88.2%
3. Departmental Head	Film and television production manager	10129	1. Media Companies (	26.9%	52.9%
3. Departmental Head	Creative Director	10131	[illegible]	28.6%	70.0%
2. Technical Leads and Specialists	Planning, process and production technicians	[illegible]	[illegible]	30.4%	10.0%
2. Technical Leads and Specialists	Software developers	[illegible]	...nology Suppliers (Hardware and Software)	33.3%	20.0%
1. Production Assistants	Business system	10114	2. Production Companies	33.3%	90.9%
2. Technical Leads and Specialists	Set designers	10146	2. Production Companies	36.4%	70.6%
1. Production Assistants	Archivists	10113	1. Media Companies (Client)	37.5%	70.0%
3. Departmental Head	Broadcasting and Entertainment Director	10133	2. Production Companies	37.5%	70.6%
			5. Niche small to medium enterprises (SME) and		

29 results