Workforce Foresighting Hub

Securing 'Tomorrow's Energy' by enabling sovereign digital security in critical national infrastructures (CNI)

A workforce foresighting study

Authors:	
Cycle Sponsor:	Northern Power Grid
Centre of Innovation:	Digital Catapult, Elise Haldane, Darren Prehaye
Workforce Foresighting Hub:	Carole Swallow

CATAPULT Digital

Powered by UKRI Innovate UK

Right skills, right time, right place

Acknowledgements

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

Skills England (formerly 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 Skills England 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 in December 2025 to March 2026 using the data set and tools available at that time.

Executive Summary

This report outlined findings from a workforce foresighting cycle focusing on **Securing 'Tomorrow's Energy' by enabling sovereign digital security in critical national infrastructures (CNI)**. This industry challenge was sponsored by Northern Power Grid, and the study was conducted by Digital Catapult in collaboration with the Workforce Foresighting Hub, an Innovate UK initiative.

Workforce foresighting is a systemic approach to forward planning that anticipates future skills and capability requirements associated with new technologies and government transformation targets. These capabilities, the actual functions a future employee can perform, can be aggregated as "future occupational profiles" (FOPs), while knowledge, skills, and behaviours (KSBs) are the more granular competences required by the profession. workforce foresighting cycles involve 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 various stakeholders to create a workforce that is prepared to effectively implement these new technologies in the sector.

Strategic context and purpose for workforce foresighting

Energy and cyber security industries are key sectors within the UK economy, strategically valuable in the defence of critical national infrastructure (CNI), promoting investment, and sustaining the transition to a net-zero economy. Together, the sectors employ approximately 226,000 staff: 158,000 working across the energy sector and 67,000 in cyber security.

With such a large workforce operating in high-risk, controlled environments, the need for new skills and upskilling to prevent and mitigate new threats from AI-equipped hackers cannot be overstated. There is widespread concern that businesses will face increasing pressures to shed jobs as AI/ML models continue to demonstrate new functionality. This will aggravate the existing risk of experienced labour exiting the market as the economy shifts towards net-zero carbon.

Contemporary cyber security adversarial exploits remain a major risk across industry: **67% of medium and 74% of large firms reported a breach within the last year**, and the National Cyber Security Centre (NCSC) was handling **four nationally significant cases per week throughout 2025**.

Partly in response, the Cyber Security and Resilience Bill will add new reporting and compliance measures, with a focus on hardening CNI and essential services.

Against this backdrop of emergent risk, persistent threats, and regulatory change, stakeholders convened a series of workshops to identify the most pressing organisational capabilities and workforce skills needed to safeguard a near-future net-zero economy.

Participants and Stakeholders

Technology Participants	Industry Participants	Skills Participants
Digital Catapult	Public Safety Communication Europe	De Montfort University, Leicester
Sunderland Software City	Hartree Centre	University of Strathclyde
	EDF Hartlepool	Anglia Ruskin University

Summary of Findings

Throughout the workshop foresighting cycle, participants identified capabilities that could strengthen the security of operational technologies (OT), a key technology component of energy related CNI, improve disaster recovery times and readiness, and better manage supply chain risk. A total of **107 capabilities** were identified across the various supply chains and types of stakeholders involved within energy CNI, reflecting upcoming job functions and responsibilities that will prove to be entirely novel. Given the current trajectory of quantum and AI/ML in business and the wider economy, the workshops concluded that the pressure to accommodate these technologies within CNI will only increase.

Employers were keen to stress the on-going risk to administrative, managerial job functions from AI, which is forcing change at considerable pace. Educators highlighted the need to update existing modules, and to allow greater specialisation in the context of continued professional development (CPD).

All workshops concluded that additional skills will be required during the next **two to five years**. Areas of particular concern were advanced operational technology (OT) security, cloud migration practices for legacy Supervisory Control and Data Acquisition (SCADA), software bill-of-materials (SBOM) uptake, and the implementation of post-quantum cryptography.

Next Steps

To deliver the proposed capabilities and equip the workforce with the requisite skills for secure and sovereign net-zero, new training pathways and specialised continued professional development (CPD) extensions for upskilling or reskilling staff are needed. Educators should review existing qualifications for cyber security provision within CNI against both the requirements for the Cyber Assessment Framework (CAF) 4.01 and the 66 unmet workforce capabilities highlighted in this report. Educators may also wish to consider liaising about the needed provisions with the UK Cyber Security Council2, as the chartered institute responsible for the Chartered Cyber Security Professional (ChCSP) standard3. Capabilities should be compared against existing cyber security apprenticeships, especially

[1] Cyber assessment framework https://www.ncsc.gov.uk/collection/cyber-assessment-framework
[2] IK Security Council https://www.ukcybersecuritycouncil.org.uk/
[3] Chartered cyber security professional https://www.ukcybersecuritycouncil.org.uk/for-individuals/become-professionally-registered/professional-titles/chartered

between education levels four and six[4], and whether more advanced provisions are necessary. Examples of priority future occupational profiles (FOPs) are detailed in section 2.2 (**2.2 Workforce Insight**) of this report, while the complete list can be found within the appendix C. (**Appendix C List of full Future Occupational Profiles**)

To accommodate emergent technologies within the provision of training for CNI, educators will need to be able to familiarise themselves with current and upcoming risks presented both to operational technology and society at large. This will require collaboration with academics, technologists, regulators, and public sector bodies to properly cognise the potential for harm, proportionality of change, and barriers to the adoption of new skills and technologies in the workforce.

[4] Education Levels https://www.gov.uk/what-different-qualification-levels-mean/list-of-qualification-levels

Glossary

Term	Definition
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.
Carbon Accounting	The process of measuring, tracking, and reporting greenhouse gas emissions produced by an organisation or activity.
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.
CPD	Continued Professional Development.
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 KSB 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.
National Challenge (Industry / Sector / Region)	A recognised technological or socio-political threat or opportunity for which there is consensus that workforce action is necessary.
Organisation Type	Simple description of nature of organisation for which capability is required.
Participants	Technologists, Educators, Employers.
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.
Roadmaps	Sector, Industry, Regional view of emerging opportunities and their market entry.
Role Group	Role groups are a collective of roles that exist in a typical manufacturing business / industrial sector.
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.

Term	Definition
Workshops	Online sessions used to undertake each step in the foresight process.
Zero-knowledge proof	Zero-knowledge proofs (ZKPs)—a method for one party to cryptographically prove to another that they possess knowledge about a piece of information without revealing the actual underlying information.
Zero-trust	Zero Trust is an IT security architectural model that requires strict identity verification for every entity, person and device attempting to access resources on a private network, regardless of whether they are sitting inside or outside of the network perimeter.

Table 1 Glossary

Table of Contents

Figures and Tables

1. Introduction

1. Introduction

1.1 Introduction to workforce foresighting

Workforce foresighting is essential in addressing the national skills challenge by aligning the skills value chain, from early education through to advanced training, with the demands of emerging technologies. By identifying future occupational profiles and the capabilities required for new roles, foresighting enables educators, employers, and policymakers to proactively adapt curricula, qualifications, and training pathways. This ensures the workforce is not only prepared for technological change but also equipped to drive innovation and productivity. In doing so, it transforms the skills gap from a reactive challenge into a strategic opportunity for national growth and resilience.

This report outlines findings from a workforce foresighting cycle focused on and titled, **Securing 'Tomorrow's Energy' by enabling sovereign digital security in in critical national infrastructures (CNI),** to safeguard CNI and enable UK national sovereignty. The study is sponsored by Northern Power Grid and conducted by Digital Catapult, in collaboration with the Workforce Foresighting Hub, an Innovate UK initiative. This report is designed to support strategic decision making and inform the next steps on the Skills Value Chain.

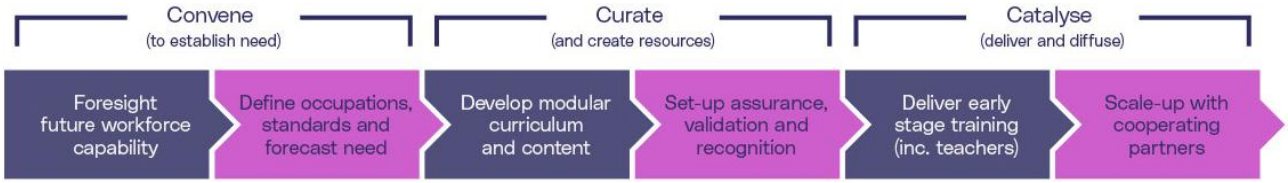

Figure 1: The Skills Value Chain (SVC)

1.2 Defining the workforce foresighting topic

Energy CNI and cyber security are strategic priorities of critical national importance, central to the support and defence of the UK economy, to the growth of business, and to accommodating the needs of the wider population. Both sectors are undergoing significant change, reflecting the commitment to a net-zero, carbon-neutral economy and the urgency of national defence in an age of geopolitical uncertainty.

Official statistics underscore the fact that cyber security is a key pillar of the UK economy, and that the energy sector is prioritising greater resilience and sovereignty to mitigate the spillover of geopolitical risk. For the period 2024 to 2025, the UK cyber security industry (Department for Science, Innovation and Technology, 2025) reported £13.2 billion in revenue, employing 67,300 staff, and growing at between 11% and 12% on the previous year. UK cyber security firms secured around £206 million in investment. In contrast, the energy sector (Department for Energy Security and Net Zero, 2025) is larger and more established, with 158,400 staff employed directly with a total of £23.6 billion invested, representing growth of 28% on the period 2023 to 2024. Energy also accounted for 8.9% of total UK investment, and 27.2% of overall industrial investment. Both sectors will remain highly strategic economic priorities as the country further shifts towards low-carbon infrastructure.

In considering which areas most warranted attention for workplace skills in energy CNI, participants were mindful of the impact of AI on the economy today, the range of surviving legacy systems in play, and governance principles to mitigate risk. Generative AI is at the forefront, owing to the scale of investment globally in market leaders, notably Anthropic, Google, and OpenAI, and the breakthrough pace of change. In the workplace, the use of office and coding assistants to automate MS Excel, Word, Outlook, as well as Visual Studio Code is fundamentally changing the nature of administrative, managerial, and engineering functions. Such change will irreversibly reshape the nature of work for millions and could have a significant impact on the size and scale of the domestic and international CNI workforce that supports the technology.

Priority themes included:

- **Sovereign cloud and on-premises architectures:**
  Data sovereignty becomes a concern where third parties can lawfully intercept information once it transgresses beyond our national boundaries (e.g. international data centres).
- **AI-enabled threat detection:**
  Automated threat detection capabilities would reduce the time needed to identify security risks and mitigate data breaches in advance.
- **SCADA transformations:**
  Migrating legacy Supervisory Control and Data Acquisition (SCADA) components to the cloud will help mitigate expense and resolve maintenance issues for outdated hardware.
- **Privacy-preserving technologies:**
  A zero-knowledge implementation, something private-by-design, makes the governance of confidential information more compliant.
- **Supply chain resilience:**
  Secure-by-design supply chains make the provenance of data and code transparent for all stakeholders to better understand any risks involved.

These topics are sufficiently broad enough to offer multiple benefits across the various stakeholders and supply chains involved in energy CNI, without overloading or overemphasising any one subsector. Taken altogether, they provide multiple layers of security and redundancy, complementing one another and improving the overall resilience of the infrastructure to a range of credible future shocks.

1.3 Contributing Participants

Thanks to all those organisations for their time and commitment to providing insights and data for this study, in the hope that this process will have a significant impact on the sector.

Technology Participants	Industry Participants	Skills Participants
Digital Catapult	Public Safety Communication Europe	De Montfort University, Leicester
Sunderland Software City	Hartree Centre	University of Strathclyde
	EDF Hartlepool	Anglia Ruskin University

Table 2: Contributing Participants

2. Findings & Insights

2. Findings and Insights

The outcomes of the three-step foresighting process were insights into three areas:

- **Industry capability insights** First, how capabilities must evolve, for the supply chain partners and 5 organisational functions that will be most impacted. Five partner types associated with the delivery of five unserved capability clusters were identified.
- **Workforce insights** Second, the occupational roles that will need to change were studied. Two role levels were identified, associated with the five supply chain partner types from Step 1. Mapping the levels into the partner types yielded 11 FOPs from which five priority areas were down selected, yielding five role types.
- **Education and training provision insights** Third, the five role types were compared against current education and training provision—using Skills England occupational standards as a benchmark—to identify where existing programmes align and where gaps exist across the organisational functions fulfilled by each role. The outcome of this analysis was a group of knowledge, skills and behaviours that are currently not provided.

This section summarises these insights, moving through organisational capabilities, to FOPs, and aligning FOPs with KSBs.

Full details of the data and findings are available in the Appendices and are accessible via the visualisation tool[5].(**Appendix**)

Introduction to the visualisation tool
The Workforce Foresighting Hub's visualisation tool is a powerful, innovative system, that 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 that 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 can be used to inform the development of future curricula 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 the detailed changes required to help update and refresh knowledge, skills and behaviours thus delivering insights for learners, providers, creators, and assurers of skills.

[5] Visualisation tool https://hvmcatapultforesighting.retool.com/embedded/public/e869283b-4b8a-437c-973e-64ab292e5b87?token=5a8879cd93ad5f696919b4149f544e96

2.1 Industry Identified Organisational Capabilities

Capabilities Identified
Exploration of organisational changes provides insights into how organisations will need to adapt their current capabilities in order to implement the solutions that respond to the challenge addressed by the foresighting project.

Insight:

The workforce challenge for securing net-zero energy systems is less about the absence of relevant technologies and more about their maturity and rate of change: while many required capabilities already exist, they sit below the readiness levels expected for CNI, and the pace of advancement—particularly in AI/ML—now significantly outstrips the capacity of current training and skills provision to adapt and keep pace.

In total, **107** capabilities were identified to support **net-zero adop**tion securely. Key themes included future cyber security principles (security-by-design, zero-knowledge), the hybridisation of SCADA (split between cloud and on-premises), secure protocols and frameworks (decentralised identifiers, digital twins), and optimisation and automation methods (model context protocols).

Most capabilities invoked technology that already exists, but at a lower technology readiness level (TRL) than CNI would typically require.[6]

For example, ~~O~~one of the technologies featured in the UK Government's Industrial Strategy (Department for Business and Trade, 2025) was Capability Hardware Enhanced RISC Instructions (CHERI), an architectural model and trusted execution environment that has significant potential, in hardening CNI against common security vulnerabilities and exploits that affect the C/C++ languages. At the time of the cycle, this technology was at the early stage of commercialisation.[7]

Across the capabilities mentioned in Appendix B, 66 were not matched to existing training provision. This partially reflects the earlier observation on the technology readiness levels (TRLs) of emerging technologies, including Capability Hardware Enhanced RISC Instructions (CHERI), that may lack sufficient commercial development to break through into current engineering workforces and training provisions. A further contributing factor is the pace of breakthrough changes in AI and machine learning, where agentic development was progressing significantly faster than anticipated, at a cadence of mere months rather than years. This difference in the TRL and pace of the respective technologies is certainly key contributing factor in technologies featuring in education provision.

A further insight from the workshops was that many new technologies, particularly AI, are being designed to assist rather than require deep technical expertise. As a result, hiring for some roles should focus less on technical versus non-technical backgrounds and more on

[6] Technology Readiness Levels (TRLs) 4–7 refer to the progression from laboratory validation (TRL 4), through validation and demonstration in relevant environments (TRLs 5–6), to prototype demonstration in an operational environment (TRL 7)
[7] Industrial Strategy https://www.gov.uk/government/collections/the-uks-modern-industrial-strategy-2025

soft skills such as critical thinking. This shift can help organisations leverage a broader range of existing talent, leading to roles being defined less rigidly and aligned more closely with the desired outcomes of each function.

Future Supply Chain

To understand how supply chains would need to evolve in response to emerging technologies, a forward-looking view of future supply chain operations was developed and compared with current practice. This comparison highlighted the areas where change was required to meet new demands and opportunities.

Throughout the process, participants identified which **supply chain partners** would be affected by the technology in question. This ensured that the analysis was grounded in real-world contexts and considered the full ecosystem of organisations involved.

The supply chain partners related to the analysis are as follows:

RTO/COI - Research & Innovation Organisations

RTO (Research and Technology Organisation) and COI (Centre of Innovation) include Catapult centres, universities, and national labs which lead low-TRL research and co-design advanced cyber security architectures, AI threat detection models, and digital skills frameworks. They drive innovation in OT/IT security and simulation platforms for workforce training.

Original Equipment Manufacturers (OEMs), Primes, Tier-1's

Major industrial automation and energy technology providers (e.g., Siemens, ABB) will manufacture secure-by-design and interoperable OT/IT hardware, embed AI and edge computing capabilities, and integrate SCADA-in-the-cloud solutions into legacy systems.

Small to Medium Enterprises

Specialist firms in cyber security, AI, IoT, and simulation will innovate niche solutions, develop bespoke integration tools, and deliver advanced training platforms. Small- and medium-sized enterprises are critical for agile development and rapid deployment of emerging technologies.

Equipment Service Providers

Managed security service providers, cloud infrastructure vendors, and system integrators will deliver secure SCADA migration, IoT connectivity, and edge computing deployments. They ensure resilience through maintenance, updates, and compliance support. They will also provide AI-enabled migrations and automation tools or kits.

Regulatory Organisations

Bodies such as Ofgem, National Cyber Security Centre (NCSC), Information Commissioner’s Office (ICO), and the UK Cyber Security Council will set and enforce standards for digital resilience, certify workforce competencies, and audit compliance with cyber and future AI regulations. They underpin trust and interoperability across the energy ecosystem as well as supply chain resilience.

The foundation of this analysis is an information architecture built around five core functional domains common to any business: **Design, Implement, Logistics, Support, and Enterprise**. These functions provided a structured lens through which shifts in capability could be assessed.

Insight:

In a Critical National Infrastructure context, the analysis showed that capability requirements were shaped by end-to-end lifecycle ownership rather than discrete functional responsibilities. Capabilities associated with CNI systems consistently spanned design, deployment, operation, and regulatory assurance, resulting in overlap across domains and reduced functional separation. This demonstrated that effective CNI resilience and security depend on integrated, lifecycle-based capability models rather than siloed interpretations of functional roles.

Capabilities were identified and mapped to pre-existing domains. For this cycle, capabilities were ultimately distributed across all five domains, however the initial technologist workshop logged no capabilities within the logistics domain. It was only after a review that the absence was noticed and rectified. The need for this correction indicated a degree of retrospective fitting (and compensation), to align capabilities across domains; the domains had already been specified and carried over from previous foresighting cycles.

Several capability clusters straddle the domains, particularly where software or hardware engineering functions required full cradle-to-grave lifecycle management, from the design and development of a solution through to its eventual sale and regulation. This reflection of the software development lifecycle, and potentially other lifecycles and supply chain processes, within the data has the effect of bulking up each domain, which is another reason why they appear to cohere so strongly.

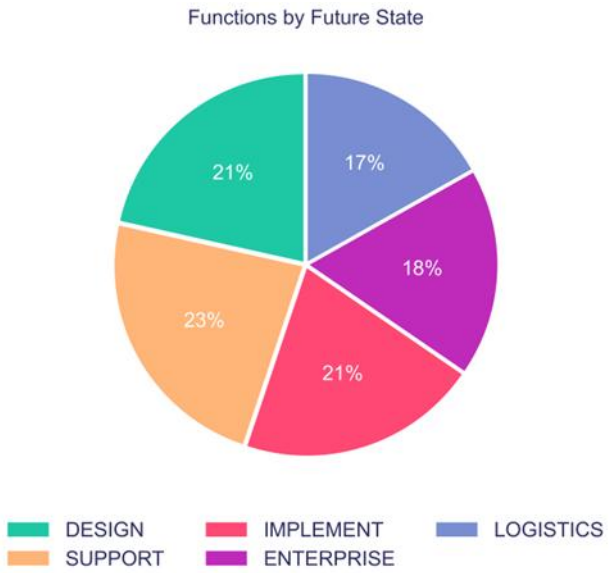

Figure 2: Future – Whole Supply Chain - Capability Function Distribution %

Links: Link to visualisation tool for **107 capabilities**[8]

By mapping these partners against the five functional domains, it was possible to identify where capability changes were required and which organisations would need to adapt, whether through new skills, new roles, or new ways of working.

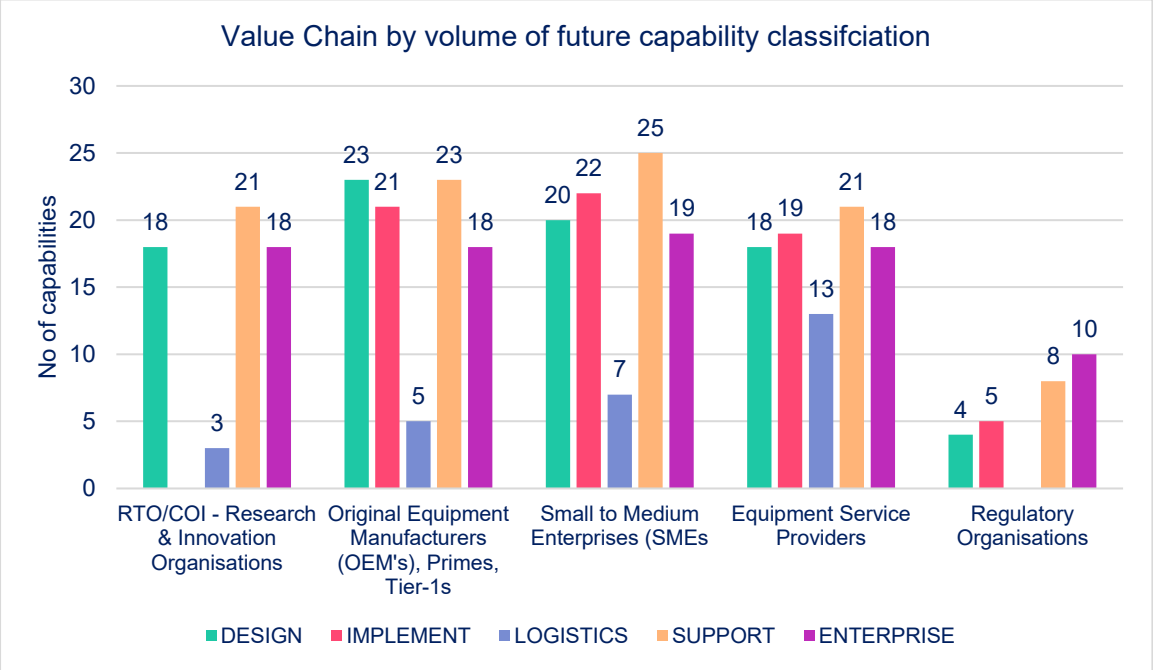

Figure 3: Distribution of Functions across each Supply Chain partner

The graph illustrates the distribution of capabilities by function across the Supply Chain Partners. These capability sets were used to inform the development FOPs within each role level.

Links: Link to visualisation tool for **5 supply chain partners**[9]

[8] https://hvmcatapultforesighting.retool.com/embedded/public/f56f84e9-8ab8-414f-aa1a-0b42ab5c71df?token=5a8879cd93ad5f696919b4149f544e96

[9] https://hvmcatapultforesighting.retool.com/embedded/public/3573002a-ab48-4fad-9765-bee00876a42e?token=5a8879cd93ad5f696919b4149f544e96

Functional Cycle Capabilities Currently Not Served

Out of the 107 future capabilities identified for this cycle to support adoption of the technology across the supply chain, 66 were not matched to any duty statements found in existing apprenticeship standards.

This finding could be indicative of a potential gap across current education and training provision, highlighting the need to develop both short and long-term training solutions to upskill the existing workforce and prepare new entrants with the skills required for securing tomorrow's energy through CNI.

The 66 unmatched capabilities were grouped into five technologies clusters, with the full list provided in Appendix B (**Appendix B Capabilities not served (unmatched) by Skills England provision).**

In the tables below, each supply chain partner type corresponds to a numbered column.

Table key:
1: RTO/COI - Research and technology organisations, communities of innovation
2: Original equipment manufacturers (OEMs)
3: Small- to medium enterprises (SMEs)
4: Equipment service providers
5: Regulatory organisations

Capability cluster 1: Sovereign cyber-security architectures for hybrid OT/IT energy systems. Capabilities grouped within this cluster focused on protecting UK energy sovereignty through secure-by-design architectures, network segmentation, cryptography, zero trust, and sovereign cloud controls. Cluster 1 included capabilities such as:

Function	Capability statement	1	2	3	4	5
SUPPORT	Implement zero-trust architectures to enhance security across critical national infrastructures	✓	✓	✓	✓	✓
SUPPORT	Implement network segmentation to isolate SCADA systems from corporate IT networks and enhance security.		✓	✓	✓	
ENTERPRISE	Establish sovereign cloud environments to ensure data sovereignty and compliance with national security regulations in critical infrastructure sectors.	✓	✓	✓	✓	✓
ENTERPRISE	Develop secure communication protocols to protect data transmission within critical national infrastructure systems.	✓	✓	✓	✓	✓
IMPLEMENT	Establish digital identities and access control protocols for devices, users, and systems across energy networks to ensure secure and verifiable interactions.		✓	✓	✓	✓

Table 3: Cluster 1 Sovereign cyber-security architectures for hybrid OT/IT energy systems.

The capabilities in this theme will strengthen national resilience by ensuring that the UK maintains control over critical energy systems in the digital age.

Capability cluster 2: AI-Enabled threat detection, surveillance and autonomous response. This cluster consolidated capabilities related to l AI-driven security, analytics, anomaly detection, and autonomous decision support capabilities. Cluster 2 included capabilities such as:

Function	Capability statement	1	2	3	4	5
SUPPORT	Integrate AI accelerators with existing critical infrastructure to improve operational resilience and performance.	✓	✓	✓	✓	
SUPPORT	Integrate AI-driven surveillance systems to enhance real-time threat detection and response in critical national infrastructure facilities.	✓	✓	✓	✓	
ENTERPRISE	Integrate artificial intelligence-driven threat detection systems to proactively identify and mitigate cyber threats in critical national infrastructures	✓	✓	✓	✓	
DESIGN	Develop interfaces for teaming between humans and AI, focusing on explicit transfer points and authority for decisions, streamlining process efficiency and accountability	✓	✓	✓	✓	
IMPLEMENT	Develop niche AI analytics tools to analyse and interpret complex data patterns within critical national infrastructure networks		✓	✓	✓	

Table 4: Cluster 2 AI-Enabled threat detection, surveillance and autonomous response.

The capabilities in this theme will enhance proactive cyber defence with intelligent systems capable of detecting and mitigating threats before they escalate.

Capability cluster 3: Secure digitalisation of SCADA, IoT and edge Infrastructure. This cluster grouped capabilities associated with IoT security, SCADA transformation, cloud migration, edge computing, and secure operational technology modernisation. Cluster 3 included capabilities such as:

Function	Capability statement	1	2	3	4	5
SUPPORT	Develop and enforce security-by-design principles to ensure IoT devices meet regulatory standards	✓	✓	✓	✓	✓
DESIGN	Integrate digital twin technologies with energy infrastructures to enhance resilience against cyber threats	✓	✓	✓	✓	
DESIGN	Design and maintain SCADA testbeds to evaluate system security and performance under simulated conditions	✓	✓	✓	✓	
ENTERPRISE	Utilize edge computing to process data locally, reducing latency and enhancing security in IoT deployments	✓	✓	✓	✓	
IMPLEMENT	Operate SCADA systems securely and resiliently in the cloud to enhance critical infrastructure operations and data accessibility		✓	✓	✓	

Table 5: Cluster 3 Secure digitalisation of SCADA, IoT and edge Infrastructure.

The capabilities in this cluster build a resilient digital foundation capable of supporting next-generation energy systems while reducing risks from increased interconnectivity. This includes the migration and transition from legacy software- and hardware-based industrial control system technologies to new hybrid cloud or multi-cloud solutions. This accommodates the risks and complexities associated with transitioning live infrastructure.

Capability cluster 4 Privacy-preserving data exchange and cryptographic security mechanisms.
This cluster captured zero-knowledge proofs, secure data-sharing protocols, privacy-enhancing technologies, and verification mechanisms. Cluster 4 included capabilities such as:

DESIGN	Develop and deploy smart contracts to automate and enforce agreements within critical national infrastructures	✓	✓	✓		
ENTERPRISE	Implement secure data-sharing protocols to facilitate confidential information exchange between energy sector organisations	✓	✓	✓	✓	✓
ENTERPRISE	Implement zero-knowledge proof protocols to verify system integrity without exposing sensitive data	✓	✓	✓	✓	
IMPLEMENT	Utilise zero-knowledge proofs to enable secure, anonymous reporting systems in critical infrastructure networks			✓		
IMPLEMENT	Establish verifiable, tamper-resistant digital identities to ensure the security and traceability of critical infrastructure assets and data		✓	✓	✓	✓

Table 6: Cluster 4 Privacy-preserving data exchange and cryptographic security mechanisms.

Capabilities within this cluster enabled trusted collaboration across the energy sector while maintaining data sovereignty and confidentiality. Novel technologies in scope include decentralised identifiers (DIDs) that can be used as cryptographic tokens to identify unique entities, typically organisations, to enhance their privacy.

Capability cluster 5: Intelligent, secure supply chain and autonomous logistics ecosystems.
This cluster integrated capabilities related to logistics security, automation suites, AI-enabled quality assurance, and secure procurement frameworks. Cluster 5 included capabilities such as:

Function	Capability statement	1	2	3	4	5
LOGISTICS	Adopt AI solutions in the assessment of quality controls compliance for products			✓	✓	
LOGISTICS	Design and validate automation suites to optimise, rationalise, and adopt component procurement strategies				✓	
LOGISTICS	Develop decision models that integrate secured logistics data to ensure reliable delivery of infrastructure components and parts to partners.				✓	
LOGICTICS	Adopt specific autonomous transport protocols to enhance logistic precision and warehouse operations efficiency		✓			
LOGISTICS	Integrate zero-knowledge protocols with enterprise resource planning systems to enhance security for logistics planning solutions			✓	✓	

Table 7: Cluster 5 Intelligent, secure supply chain and autonomous logistics ecosystems.

Capabilities within this cluster reinforced the resilience of the energy supply-chain, which was critical to maintaining uninterrupted, secure national energy operations. This cluster incorporates autonomous, more humanoid robots and other automated forms of cyber-

physical system, reflecting the need for safe physical interactions with infrastructural components.

Prioritised capability themes

Across the supply chain partners in this foresighting cycle, a total of 107 capabilities were identified. Following review and validation with the expert participants, a subset of these capabilities was prioritised as critical for the successful adoption of a cross-disciplinary cyber security workforce capable of protecting increasingly complex systems.

This prioritisation was based specifically on the capabilities assessed as essential within Survey B, which asked participants across all stakeholder groups to evaluate the importance of each capability for future implementation readiness. The analysis focused specifically on those capabilities required to support secure adoption, operational resilience, and regulatory assurance within a critical national infrastructure context.

From this analysis, four priority capability themes were derived. These themes bring together individual essential capabilities into broader areas of strategic importance for the transition to advanced digital competency, reinforcing the UK's energy sovereignty in the digital age. Each theme represents a cluster of related technical, regulatory, or organisational competencies that must be strengthened to remove barriers to adoption, support regulatory confidence, and enable operational excellence.

Top 4 Priority capability themes

- **Cyber security strategies for critical national infrastructure**
- **SCADA system security and cloud migration**
- **Advanced security protocols and frameworks**
- **Optimisation and automation in energy sector**

Insight:

The convergence of legacy OT, hybridised SCADA, cloud platforms, and emerging quantum-era threats is accelerating cyber risk across critical national infrastructure beyond the capacity of current security architectures and governance models.

Although strategies such as zero-trust, sovereign cloud, advanced assurance mechanisms, and AI/ML-enabled security are increasingly adopted, their effectiveness is constrained by misconfiguration risk, limited workforce capability, and reduced interpretability in high-integrity systems.

As a result, cyber security in a quantum context is fundamentally a system-design and human-oversight challenge, requiring secure-by-default architectures, coherent governance across IT/OT and supply chains, and targeted capability development to avoid increasing operational fragility during modernisation.

Cyber security strategies

This theme covered the design and governance of end-to-end strategies for CNI, specifically operational technology, IT, cloud platforms, and supply chains. Its inclusion reflected the prevalence of malicious attacks, accidental disclosure, and the rate at which new vulnerabilities are discovered, all of which point to a need for greater strategic direction around secure designs and defaults and the minimisation of risk at scale. Examples associated with this theme included zero-trust architectures, network segmentation,

sovereign cloud environments, secure identity and access management, disaster recovery, and compliance with evolving cyber-resilience obligations.

SCADA system security and cloud migration

SCADA was identified as a standalone theme owing to its operational value and the fact that, as a legacy high-integrity CNI system, it had become misaligned with modern requirements for greater resilience and maintainability. The focus of this theme was therefore on the hybridisation of SCADA, securing systems by migrating selected functions to the cloud, to create hybrid or multi-cloud architectures. Risks for hybridised SCADA include misconfiguration, the loss of determinism and sovereign control, an expanded attack surface, and the inadequacy of subsequent non-functional testing, be it load (or throughput), performance, or security.

Advanced security protocols and frameworks

This theme was a broad collection of novel practices unmet within the workforce today, specifically post-quantum cryptography, verifiable digital identities, zero-knowledge proofs, and software bill-of-materials (SBOMs). These techniques functioned as sophisticated assurance and provenance mechanisms intended to demonstrate the resilience of credentials and key infrastructure (PQC), surety about the identity of companies within a supply chain and the reduction of confidential (proprietary) data available to them, and detail on potential vulnerabilities or obsolescence within a supplier’s own software products (SBOMs). Common risks with the adoption of advanced security protocols and techniques are the shortage of skills to implement each correctly, the challenge of integrating them, and the risk of misinterpreting the assurances they were designed to provide.

AI/ML optimisation and automation in the energy sector

This final theme may straddle the other three to the greatest degree, with AI and machine learning agents being relied on increasingly to design, implement, and verify the above. AI/ML-driven optimisation and automation comprise power system algorithms used to monitor performance, the intrusion detection and prevention heuristics that detect hackers, and routines for predictive maintenance and decision-making. A common drawback to the intensification of AI/ML models was the opacity of decision-making itself and the subsequent lack of interpretability, or explanatory power, where the workforce is left unable to attribute the actual reason for the algorithm's outcomes. At its heart, contemporary AI/ML solutions rely primarily on pattern-matching algorithms that predict the next word or symbol in a sequence. Misconceptions about what the models are, or will be, capable of achieving could lead to misalignment and the de-skilling of human labour precisely when greater care and control is needed, particularly for high-integrity systems.

2.2 Workforce Insight

Future Occupational Profiles

FOPs indicated how roles within industry were expected to evolve as the nature of the technology changes, to become more automated, secure, and resilient. They defined the key responsibilities, knowledge, skills, and behaviours required for each role, to ensure alignment with ongoing industrial transformation.

The FOPs defined for this cycle do not seek to represent the full scope of current or future job role. Instead, the workforce foresighting process identified new capabilities and capability shifts required within an occupation in the future to enable technology adoption.

Links: Link to **FOP Matrix**[10]

As part of the strategic workforce planning undertaken through this cycle, FOPs were identified and prioritised based on a defined set of key criteria. A Priority FOP, however, is defined as a role that is critical to our future success and must be developed ahead of others to meet evolving business needs.

These roles are prioritised because they were strategically important to the sectors' long-term goals

- Faced current or anticipated capability gaps
- Had a high impact across multiple functions
- Required early talent planning and pipeline development
- Needed to be ready within a defined timeframe

Role Levels

Organisations relied on structured role levels to manage talent, drive performance and support sustainable growth. A clear hierarchy from entry level to executive leadership ensures responsibilities are well defined and expectations aligned. Each level builds on the last in terms of complexity, autonomy and impact, enabling effective collaboration and accountability.

In workforce foresighting, the same role levels are used across Supply Chain Partners for a given technology and defined within this context. This shared framework supported consistency, clarity of FOPs and associated capability development both within and between sectors. Each workforce foresighting challenge defined role levels that reflect the requirements of the challenge and sector.

Role Levels for this cycle are:

1. **Professional and Delivery**
   Execution and Tactical Delivery: Analyse within defined systems.
2. **Strategic & Operational Management**
   Lead teams, assess systems, design solutions and manage resources.

[10] https://hvmcatapultforesighting.retool.com/embedded/public/f99a913f-8827-4730-8893-d618d489bc84?token=5a8879cd93ad5f696919b4149f544e96

Future Occupational Profiles results

To enable sovereign digital security in CNI, 11 FOPs were identified. These FOPs are presented below, by role level and across the identified supply chain partners.

Role Level	FOP	RTO/COI-Research & Innovation Organisations	Original Equipment Manufacturers (OEMs), Primes, Tier-	Small to Medium Enterprises (SMEs)	Equipment Service providers	Regulatory Organisations
Strategic & Operational Management	IT Information Manager	✓	✓	✓	✓	✓
	Lifecycle Risk Managers	✓	✓	✓	✓	✓
	Manager in Logistics		✓	✓	✓	
Professional & Delivery	Compliance & Regulatory Professionals	✓	✓	✓	✓	✓
	Data Architects	✓	✓	✓	✓	✓
	Data Engineers	✓	✓	✓	✓	
	Dev Ops Engineers	✓	✓	✓	✓	
	IT Quality & Testing Professionals	✓	✓	✓	✓	
	Mechatronic Engineers	✓	✓	✓	✓	
	Power Systems Engineers	✓	✓	✓	✓	
	Security Controls & Instrumentation Engineer	✓	✓	✓	✓	

Table 8: FOP by Role Level and supply chain partner

Priority FOPs

The FOPs were reviewed by expert cycle participants against the context of importance to the sector, demand, mapping and alignment against existing education and training provision. The following FOPs have been prioritised for initial action and further analysis. The FOPs outlined below have been identified as key roles within the future workforce, essential for delivering the capabilities required to enable a cross-disciplinary cyber-security workforce capable of protecting increasingly complex systems.

Insight:

The prioritised Future Occupational Profiles reflect a shift towards sovereign, secure-by-design digital operations within Critical National Infrastructure, requiring the convergence of IT, OT, and cyber-security roles to deliver resilient, auditable, and compliant systems capable of operating securely at national scale.

The following FOPs have been prioritised for this cycle because they represent the most critical roles needed to enable sovereign digital security in CNI). These future occupational profiles reflect the shift towards sovereign, secure-by-design digital operations across Critical National Infrastructure. DevOps, IT, power systems, and SCADA/controls engineers will evolve into architects of resilient cloud-SCADA ecosystems—integrating zero-trust security, interoperable data frameworks, AI-enabled monitoring, and automated, auditable pipelines. Together, they will enable predictive, cyber-resilient, low-latency energy and infrastructure operations, ensuring uninterrupted, compliant, and sovereign service across the UK's most critical systems.

- DevOps Engineer
- IT Architects
- IT Engineers
- Power Systems Engineers
- Security Controls and Instrumentation manager

DevOps Engineer

It embeds verifiable security and operational control end-to-end, keeping telemetry and decision rights within sovereign boundaries while reducing the attack surface and ensuring resilient, compliant, uninterrupted service.

IT Architect

Architecture is where sovereignty is enforced—it sets the reference models, controls, and data-sharing guardrails that deliver verifiable integrity, least-privilege access, vendor independence, and compliant cross-organisation interoperability.

IT Engineer

It operationalises sovereignty and security every day—detecting anomalies early, maintaining configuration integrity, and ensuring low-latency control and recovery within the sovereign perimeter.

Power Systems Engineer

It safeguards the energy backbone by maintaining sovereign command over grid models and operations, reducing systemic risk while balancing security, stability, and decarbonisation objectives.

Security Controls and Instrumentation Manager
It hardens the sensing and actuation layer where cyber events become physical, ensuring telemetry, calibration, and control remain trustworthy, traceable, and under sovereign authority.

Links: Links to Appendix C (**Appendix C List of full Future Occupational Profiles**) and full details on FOPs versus provision. **visualisation tool for 11 FOPs**[11]

[11] FOPs vs Provision https://hvmcatapultforesighting.retool.com/embedded/public/d9f485a2-6d23-45dd-ab48-4c4c87ced0c7?token=5a8879cd93ad5f696919b4149f544e96

2.3 Education &Training provision insights

2.3.1 Provision Analysis of FOPs and Capabilities

The tables below provide a comparison of each priority FOP against the highest scoring existing education provision. They identified the highest-scoring standard for each profile and highlighted capabilities that are not currently addressed by the selected apprenticeship standard. These unmet capabilities informed potential areas for future development of education and training provision, either by adapting existing programmes or through the creation of short CPD courses aimed at upskilling the current workforce.

DevOps Engineer

Key Tasks: Governs secure-by-design SCADA-to-cloud operations by designing testbeds and hybrid prototypes, codifying commissioning checklists and acceptance tests, implementing segmentation and zero-trust, engineering AI-driven monitoring, and running automated, auditable CI/CD with rollback to ensure resilient, compliant, uninterrupted service.

Aligned to supply chain partners: Original Equipment Manufacturers (OEM's), Primes &Tier-1s, Small to Medium Enterprises (OEMs), RTO/CTI-Research & Innovation Organisations, Equipment Service Providers, Regulatory Organisations.

In FOP vs Provision there was a 7% fit with Skills England **Dev Ops Engineer Standard**[12]. The unmatched FOP capabilities are shown in the table below:

Function Area	Capability Statement
DESIGN	Develop interfaces for teaming between humans and AI, focusing on explicit transfer points and authority for decisions, streamlining process efficiency and accountability
DESIGN	Develop analytics tools for monitoring and analysing specific critical infrastructure networks to enhance their security and performance.
DESIGN	Design and maintain SCADA testbeds to evaluate system security and performance under simulated conditions.
DESIGN	Develop hybrid SCADA prototypes to validate interoperability between cloud-based services and existing operational technology systems.
DESIGN	Develop AI-driven threat detection algorithms to identify and mitigate cyber threats in critical national infrastructure systems.
DESIGN	Develop zero-trust architectures for critical national infrastructures to enhance cybersecurity resilience.
SUPPORT	Integrate MCP with existing security frameworks to strengthen resilience against cyber threats in energy sector infrastructures.
SUPPORT	Deploy a tailored AI-driven customer support system that utilizes chatbots and voice assistants to enhance user interaction and support.
SUPPORT	Integrate AI-driven surveillance systems to enhance real-time threat detection and response in critical national infrastructure facilities.
SUPPORT	Integrate AI accelerators with existing critical infrastructure to improve operational resilience and performance.
SUPPORT	Design secure network architectures for critical infrastructure to prevent unauthorized access and ensure system resilience.
SUPPORT	Develop SCADA migration strategies to ensure secure and efficient transition to cloud environments.

[12] Dev Ops Engineer standard https://skillsengland.education.gov.uk/apprenticeships/st0825-v1-1

Function Area	Capability Statement
SUPPORT	Implement zero trust architectures to enhance security across critical national infrastructures.
ENTERPRISE	Implement zero-knowledge proof protocols to verify system integrity without exposing sensitive data.
ENTERPRISE	Implement AI-driven anomaly detection to identify and mitigate cyber threats in critical national infrastructure.
ENTERPRISE	Develop software and AI tools for detecting and preventing security threats.
ENTERPRISE	Integrate artificial intelligence-driven threat detection systems to proactively identify and mitigate cyber threats in critical national infrastructures.
IIMPLEMENT	Develop and implement network segmentation strategies to isolate operational technology systems from information technology networks, enhancing security and reducing attack surfaces.
IMPLEMENT	Develop integration solutions between multiple cloud platforms and original equipment manufacturers to enhance system resilience and data accessibility.
IMPLEMENT	Implement critical national infrastructure grade SCADA-in-the-cloud specific security solutions to enhance operational efficiency and scalability.
IMPLEMENT	Install AI monitoring tools to continuously oversee and assess the security posture of critical national infrastructure components.
IMPLEMENT	Operate SCADA systems securely and resiliently in the cloud to enhance critical infrastructure operations and data accessibility.
IMPLEMENT	Establish secure testbeds for SCADA migration to validate system performance and security before deployment.
IMPLEMENT	Develop SCADA migration utilities to facilitate seamless transition from legacy systems to modern platforms.
LOGISTICS	Integrate zero-knowledge protocols with enterprise resource planning systems to enhance security for logistics planning solutions.
LOGISTICS	Design and validate automation suites to optimise, rationalise, and adopt component procurement strategies
LOGISTICS	Commission checklists and perform acceptance tests to ensure efficient deployment of hardware and software elements.
LOGISTICS	Implement secure automated pipelines for onboarding specialised cyber-physical systems, with mechanisms to effect different rollback strategies.

Table 9: DevOps Engineer FOP capabilities not served by Skills England

IT Architects

Key Tasks: Designs and governs sovereign, secure-by-design digital estates by instituting zero-trust, verifiable SBOMs, tamper-resistant AI, and zero-knowledge protocols; defining secure cloud patterns and interoperable standards; architecting SCADA-to-cloud migration with secure identities and auditable pipelines; and delivering decision-support interfaces that sustain resilience.

Aligned to supply chain partners: Original Equipment Manufacturers (OEM's), Primes &Tier-1s, Small to Medium Enterprises (OEMs), RTO/CTI-Research & Innovation Organisations, Equipment Service Providers, Regulatory Organisations.

In FOP vs Provision there was an 6% fit with Skills England Cyber Security Technologist Standard[13]. The unmatched FOP capabilities are shown in the table below:

Function Area	Capability Statement
DESIGN	Develop interoperability frameworks for critical national infrastructure to ensure secure data exchange between different systems.
DESIGN	Develop zero-trust architectures for critical national infrastructures to enhance cybersecurity resilience.
DESIGN	Design security interfaces and decision-support tools to enable rapid, safe, and informed actions by critical national infrastructure activities.
DESIGN	Design governance mechanisms for AI-enabled systems to ensure auditability and decision accountability.
DESIGN	Develop and implement zero-knowledge proof protocols for specific critical national infrastructure systems to improve data privacy and ensure robust security measures.
SUPPORT	Utilize tamper-proof AI models to maintain the integrity and availability of critical national infrastructure systems.
SUPPORT	Implement network segmentation to isolate SCADA systems from corporate IT networks and enhance security.
SUPPORT	Develop interoperable data standards to facilitate seamless and secure cross-organisational data sharing.
SUPPORT	Develop SCADA migration strategies to ensure secure and efficient transition to cloud environments.
SUPPORT	Design secure cloud platforms to support scalable and resilient energy management services.
SUPPORT	Develop tamper-proof AI systems to maintain data integrity and prevent unauthorized modifications in critical infrastructures.
SUPPORT	Implement zero trust architectures to enhance security across critical national infrastructures.
SUPPORT	Develop interoperability frameworks to integrate legacy systems with modern digital security protocols.
SUPPORT	Implement sovereign digital platforms to secure AI and cloud infrastructures within national borders.

[13] Cyber Security Technical Professional (integrated degree)
https://skillsengland.education.gov.uk/apprenticeships/st1021-v1-1

Function Area	Capability Statement
ENTERPRISE	Implement secure data exchange protocols to facilitate safe and efficient cross-organisation data sharing.
ENTERPRISE	Develop secure MCP client-server architectures to enhance data integrity and confidentiality in critical national infrastructures.
ENTERPRISE	Establish sovereign cloud environments to ensure data sovereignty and compliance with national security regulations in critical infrastructure sectors.
ENTERPRISE	Implement secure data-sharing protocols within dashboards to ensure compliance with national cybersecurity regulations for critical national infrastructure.
ENTERPRISE	Develop secure communication protocols to protect data transmission within critical national infrastructure systems.
ENTERPRISE	Implement secure data-sharing protocols to facilitate confidential information exchange between energy sector organisations.
IMPLEMENT	Integrate tamper-resistant transaction and audit mechanisms to support secure energy markets and fraud detection.
IMPLEMENT	Develop integration solutions between multiple cloud platforms and original equipment manufacturers to enhance system resilience and data accessibility.
IMPLEMENT	Establish verifiable, tamper-resistant digital identities to ensure the security and traceability of critical infrastructure assets and data.
IMPLEMENT	Establish zero trust architectures to ensure secure communication and access control within IoT-enabled energy networks.
LOGISTICS	Integrate zero-knowledge protocols with enterprise resource planning systems to enhance security for logistics planning solutions.
LOGISTICS	Develop decision models that integrate secured logistics data to ensure reliable delivery of infrastructure components and parts to partners.
LOGISTICS	Operate secure-by-design integration, delivery, and maintenance chains to ensure consistent system reliability and security compliance.
LOGISTICS	Implement secure automated pipelines for onboarding specialised cyber-physical systems, with mechanisms to effect different rollback strategies.
LOGISTICS	Design and validate zero-knowledge protocols within ERP and logistics planning solutions
LOGISTICS	Create a verifiable bill of materials for hardware and software components to ensure accurate tracking and maintenance.

Table 10: IT Architects FOP capabilities not served by Skills England

IT Engineers

Key Tasks: Engineers secure-by-design, AI-enabled infrastructure by establishing QA drift baselines and predictive maintenance, building secure cloud deployments, implementing secure interoperable MCP interactions, deploying hybrid SCADA prototypes, implementing interoperability standards, developing edge AI analytics and anomaly detection, and operating cloud SCADA or edge infrastructure with automated, auditable pipelines and rollback for low latency, uninterrupted service.

Aligned to supply chain partners: Original Equipment Manufacturers (OEM's), Primes &Tier-1s, Small to Medium Enterprises (OEMs), RTO/CTI-Research & Innovation Organisations, Equipment Service Providers, Regulatory Organisations.

In FOP vs Provision there was an 9% fit with Skills England Cyber Security Technical Professional (integrated degree) Standard. The unmatched FOP capabilities are shown in the table below:

Function Area	Capability Statement
DESIGN	Develop advanced cryptographic authentication mechanisms to securely bind digital twins to their corresponding physical assets.
DESIGN	Develop hybrid SCADA prototypes to validate interoperability between cloud-based services and existing operational technology systems.
DESIGN	Develop interoperability frameworks for critical national infrastructure to ensure secure data exchange between different systems.
ENTERPRISE	Utilize edge computing to process data locally, reducing latency and enhancing security in IoT deployments.
ENTERPRISE	Implement secure data-sharing protocols to facilitate confidential information exchange between energy sector organisations.
IMPLEMENT	Develop niche AI analytics tools to analyse and interpret complex data patterns within critical national infrastructure networks.
IMPLEMENT	Develop edge AI solutions to enable on-device data processing for improved security and efficiency in energy systems.
IMPLEMENT	Integrate edge computing solutions to enhance real-time data processing and operational efficiency in energy systems.
IMPLEMENT	Integrate tamper-resistant transaction and audit mechanisms to support secure energy markets and fraud detection.
IMPLEMENT	Operate SCADA systems securely and resiliently in the cloud to enhance critical infrastructure operations and data accessibility.
IMPLEMENT	Utilise zero-knowledge proofs to enable secure, anonymous reporting systems in critical infrastructure networks.
LOGISTICS	Develop decision models that integrate secured logistics data to ensure reliable delivery of infrastructure components and parts to partners.
LOGISTICS	Demonstrate the application of zero-knowledge protocols within ERP and logistics planning solutions
LOGISTICS	Integrate automation suites to optimise, rationalise, and adopt component procurement strategies

Function Area	Capability Statement
LOGISTICS	Integrate AI solutions into the software used for checking product availability to enhance logistics processes.
LOGISTICS	Implement secure automated pipelines for onboarding specialised cyber-physical systems, with mechanisms to effect different rollback strategies.
SUPPORT	Design secure cloud platforms to support scalable and resilient energy management services.
SUPPORT	Develop interoperable data standards to facilitate seamless and secure cross-organisational data sharing.
SUPPORT	Integrate AI-enhanced anomaly detection to monitor and secure critical infrastructure systems against potential disruptions.

Table 11: IT Engineers FOP capabilities not served by Skills England

Power Systems Engineers

Key Tasks: Optimises energy systems with AI and advanced modelling by analysing demand/generation to maximise low-carbon utilisation, integrating digital twins for cyber-resilient planning, deploying edge computing and secure remote control, and ensuring stable, efficient, sovereign grid operations

Aligned to supply chain partners: Original Equipment Manufacturers (OEM's), Primes &Tier-1s, Small to Medium Enterprises (OEMs), RTO/CTI-Research & Innovation Organisations, Equipment Service Providers.

In FOP vs Provision there were no fits with Skills England apprenticeships. The unmatched FOP capabilities are shown in the table below:

Function Area	Capability Statement
DESIGN	Integrate digital twin technologies with energy infrastructures to enhance resilience against cyber threats.
DESIGN	Develop interoperability frameworks for critical national infrastructure to ensure secure data exchange between different systems.
IMPLEMENT	Analyse facility energy demands and generation constraints to maximise the efficient utilisation of low carbon energy sources in specific operational sectors.
IMPLEMENT	Integrate assets and grid interfaces to improve efficiency, stability and renewable energy utilisation
IMPLEMENT	Using advanced computational modelling techniques to optimize energy generation processes.
IMPLEMENT	Integrate secure, resilient, and safety-governed remote control of electrical networks to support efficient operation.
IMPLEMENT	Integrate edge computing solutions to enhance real-time data processing and operational efficiency in energy systems.

Table 12: Power Systems Engineers FOP capabilities not served by Skills England

Security Controls and Instrumentation Engineer

Key Tasks: Governs secure, AI-enabled SCADA/IoT by deploying ML-based predictive maintenance, designing SCADA testbeds and hybrid prototypes to validate security, performance, and interoperability, engineering security controllers/HMIs and decision-support tools, leading sensor prototyping/migration/calibration, integrating digital twins, and maintaining research-grade SCADA for resilient remote control

Aligned to supply chain partner: Original Equipment Manufacturers (OEM's), Primes &Tier-1s, Small to Medium Enterprises (OEMs), RTO/CTI-Research & Innovation Organisations, Equipment Service Providers.

In FOP vs Provision there were no fits with Skills England apprenticeships. The unmatched FOP capabilities are shown in the table below:

Function Area	Capability Statement
DESIGN	Design and maintain SCADA testbeds to evaluate system security and performance under simulated conditions.
DESIGN	Design security interfaces and decision-support tools to enable rapid, safe, and informed actions by critical national infrastructure activities.
DESIGN	Test IoT-enabled sensors to validate data collection accuracy and support predictive maintenance strategies.
DESIGN	Develop hybrid SCADA prototypes to validate interoperability between cloud-based services and existing operational technology systems.
DESIGN	Develop hardware solutions with industry partners to enhance security for critical national infrastructure, specifically by implementing Trusted Execution Environment technologies.
DESIGN	Develop advanced cryptographic authentication mechanisms to securely bind digital twins to their corresponding physical assets.
DESIGN	Develop and deploy smart contracts to automate and enforce agreements within critical national infrastructures.
SUPPORT	Maintain research-grade SCADA systems to support continuous innovation and development in critical infrastructure.
SUPPORT	Deploy AI-based predictive maintenance systems to proactively identify and address vulnerabilities in critical infrastructure components.
SUPPORT	Integrate MCP with existing security frameworks to strengthen resilience against cyber threats in energy sector infrastructures.
SUPPORT	Design secure network architectures for critical infrastructure to prevent unauthorized access and ensure system resilience.
SUPPORT	Integrate AI-driven surveillance systems to enhance real-time threat detection and response in critical national infrastructure facilities.
SUPPORT	Implement network segmentation to isolate SCADA systems from corporate IT networks and enhance security.
SUPPORT	Utilise AI-based forensic analysis to investigate and respond to cyber incidents affecting critical infrastructure.
ENTERPRISE	Integrate artificial intelligence-driven threat detection systems to proactively identify and mitigate cyber threats in critical national infrastructures.
ENTERPRISE	Implement AI-driven anomaly detection to identify and mitigate cyber threats in critical national infrastructure.

Function Area	Capability Statement
ENTERPRISE	Implement zero-knowledge proof protocols to verify system integrity without exposing sensitive data.
ENTERPRISE	Encrypt data in transit and at rest to protect sensitive information within IoT networks.
IMPLEMENT	Design security controllers for critical national infrastructure SCADA systems to improve specific operational metrics and guarantee consistent system performance.
IMPLEMENT	Integrate secure, resilient, and safety-governed remote control of electrical networks to support efficient operation.
IMPLEMENT	Integrate digital twins with IoT systems to enhance real-time monitoring and predictive maintenance of energy assets.
IMPLEMENT	Integrate tamper-resistant transaction and audit mechanisms to support secure energy markets and fraud detection.
IMPLEMENT	Utilise zero-knowledge proofs to enable secure, anonymous reporting systems in critical infrastructure networks.
LOGISTICS	Implement chain of custody procedures to ensure secure handling of hardware and deploy calibration procedures to maintain accuracy in measurements.
LOGISTICS	Demonstrate the application of zero-knowledge protocols within ERP and logistics planning solutions

Table 13: Security Controls and Instrumentation Engineer FOP capabilities not served by Skills England

FOPs with the biggest Education provision gaps

The table below lists the full set of FOPs defined for this foresighting cycle. It highlighted gaps in existing provision by identifying the best fit existing apprenticeship standard, based on Maximum Fit Factor. The Maximum Fit Factor is combined with the Surplus Factor to determine the Apprenticeship Suitability score of Low, Medium or High.

A detailed comparison of existing apprenticeship provision against the capability requirements of the identified FOPs is available in the data visualisation tool: **FOP vs Provision[14].**

Table Key:
1. RTO/COI - Research & Innovation Organisations
2. Original Equipment Manufacturers (OEM's), Primes, Tier-1s
3. Small to Medium Enterprises (SMEs)
4. Equipment Service Providers
5. Regulatory Organisations

[14] FOP vs Provision https://hvmcatapultforesighting.retool.com/embedded/public/d9f485a2-6d23-45dd-ab48-4c4c87ced0c7?token=5a8879cd93ad5f696919b4149f544e96

Role Level	FOP Title	Required for SCPs	Best Fit Apprenticeship Standard/s	Apprenticeship Suitability[15]
Strategic & Operational Management	IT Information Managers	1,2,3,4,5	Cyber security technologist (11%)	LOW
	Lifecycle Risk Managers	1,2,3,4,5	Cyber security technologist (50%)	MEDIUM
	Managers in Logistics	2,3,4	None	-
Professional and Delivery	Compliance and Regulatory Professionals	1,2,3,4,5	Machine learning engineer (21%)	LOW
	DevOps Engineers	1,2,3,4,5	DevOps Engineer (7%)	LOW
	IT Architects	1,2,3,4,5	Machine learning engineer (12%)	LOW
	IT Engineers	1,2,3,4,5	Cyber security technologist (9%)	LOW
	IT Quality and Testing Professionals	1,2,3,4	None	-
	Mechatronic Engineers	1,2,3,4	Robotics engineer – degree (29%)	LOW
	Power Systems Engineers	1,2,3,4	Electrical power networks engineer (28%)	LOW
	Security Controls and Instrumentation Engineer	1,2,3,4	Digital manufacturing engineering leader (12%)	LOW

Table 14: FOP vs Closest Existing Apprenticeship (Skills England) Provision

Links: Link to **FOP Distribution**[16]

[15] Suitability /Fit Factor is determined based on semantic matching between the capability statements within a profile and the duty statements within an apprenticeship profile. 100% would indicate a match above the threshold for linguistic matching, for all capabilities within a FOP

[16] FOP distribution https://hvmcatapultforesighting.retool.com/embedded/public/ce67cca1-5beb-4557-8482-8a0b6e174933?token=5a8879cd93ad5f696919b4149f544e96

2.3.2 Knowledge, Skills, and Behaviour tags and its observations.

For each capability in a foresighting cycle, a team of expert educators have determined the relevant KSBs required by the workforce to deliver the capability. This approach enables two key use cases:

1. **Informing / Guiding understanding of the alignment between future-state capability requirements and current educational provision.**
2. **Driving action by equipping educators to embed these capabilities into their curriculum.**

While capabilities define what organisations required to thrive in the future, KSBs provide a practical framework for how education needed to evolve to support that transformation. Capability tags that aligned well with current educational provisions also revealed shifts in KSBs requirements. Capabilities introduced during the cycle were similarly associated with relevant tags that will support educators to integrate those capabilities into curriculum effectively.

This intersection between capability relevance and knowledge, skills and behaviour (KSB) evolution was critical for identifying where curriculum updates were required to keep pace with industry transformation.

Application

The complete list of KSBs associated with each capability was available within the visualisation tool, alongside all other relevant contextual information.

The application of this data can be broadly divided into two key areas:

1. **Macro Trend Analysis**
   By examining KSB tags at an aggregate level across all capabilities, educators were able to identify major shifts in demand. This high-level view helped narrow the focus to areas where change is most significant or emerging.

2. **Detailed Research**
   Once priority areas had been identified through the macro lens, educators were able to drill down into specific capabilities or explore the detailed KSBs linked to a particular tag. This supported more targeted curriculum development and informed decision-making.

This report presents a selection of aggregated insights intended to illustrate potential use cases. Readers are strongly encouraged to explore the visualisation tool for a more detailed and interactive engagement with the data. The tool offers deeper context, flexible filtering, and access to the full range of capabilities and KSB tags, enabling users to tailor their exploration to specific interests or needs.

Most frequent tags

The following graphic highlights the most frequently used tags across all capabilities in the foresighting cycle. These tags reveal macro trends that can guide the focus of training provisions.

Most frequent Knowledge Tags

Tag	Tag Frequency
Artificial Intelligence (AI)	23
Information Security	22
Security Engineering	20
System Integration	19
Computer And Information Security	13
SCADA (Supervisory Control and Data Acquisition)	11
Cyber Threat Intelligence	10
Cloud Computing	8
Cryptography	8
Intrusion Detection Systems	8
Internet of Things (IoT)	6
Computer Security	5
Regulatory Compliance	5
Supply Chain Security	5
System Testing	5
Threat Assessment	5

Table 15: Most frequent Knowledge Tags

Most frequent Skills Tags

Tag	Tag Frequency
Integrate systems and software	22
Identify and manage cybersecurity threats	20
Conduct cyber security risk assessments	19
Monitor security of digital information	18
Secure and monitor network access	11
Gather and analyse cyber threat intelligence	10
Implement cryptographic tools in applications	8
Configure SCADA packages	7
Develop information security policies	7
Use machine learning to create or improve solutions	7
Guide AI tools to process and transform data	6
Implement and manage cloud infrastructure	6
Guide AI tools to analyse and interpret data	5
Manage IT legacy system integration	5
Use safety critical communication protocols	5

Table 16: Most frequent Skills Tags

This data also served as an early signal of emerging knowledge and skill areas, enabling readers to use the visualisation tool to explore capability- or FOP-specific KSB in greater detail.

2.4 Priority evaluation of underserved and high-demand capability themes

Educators conducted a targeted review of capability statements and FOPs to identify areas where there is:

- High forecasted demand for specific capabilities in the future workforce, and
- Low current curriculum coverage, meaning these capabilities are not adequately addressed in existing educational programmes.

By focusing on this intersection of high demand but underserved provision, educators were able to identify critical capability gaps that may hinder workforce readiness if left unaddressed. This approach supported strategic curriculum development by highlighting which capabilities should be prioritised for inclusion or enhancement in training programmes.

Discussion

Several capability clusters emerged from the clustering of capability statements by high demand and low existing provision. These clusters reflected areas where current educational offerings were not sufficient to prepare learners for future roles, particularly in sectors undergoing rapid transformation. The following clusters represent key capability gaps and proposed solutions:

- **Cluster 1:** Sovereign cyber-security architectures for hybrid OT/IT energy systems.
- **Cluster 2:** AI-Enabled threat detection, surveillance and autonomous response.
- **Cluster 3:** Secure digitalisation of SCADA, IoT and edge Infrastructure.
- **Cluster 4:** Privacy-preserving data exchange and cryptographic security mechanisms.
- **Cluster 5**: Intelligent, secure supply chain and autonomous logistics ecosystems.

These themes highlight a shift in workforce capability requirements towards sustainability, strategic thinking, and interdisciplinary collaboration. Addressing these gaps will require coordinated efforts between educators, industry partners, and curriculum designers to ensure future professionals are equipped for evolving occupational demands.

3. Conclusion & Next Steps

3. Conclusions and Next Steps

To drive meaningful transformation across the target sectors, strong leadership, strategic investment, and a deep understanding of emerging innovations are essential. Our analysis underscores the importance of aligning workforce development with future demands, particularly through the adaptation of apprenticeship and degree programmes and the creation of flexible CPD opportunities. These efforts will ensure that individuals are equipped with the skills and knowledge required to navigate evolving technologies and practices.

3.1 Key Findings & Conclusions

From the workforce foresighting cycle the following data points were identified and focus areas were developed.

Key Findings

Future Capabilities & Roles: 107 future capabilities were identified with 75 newly defined, leading to 11 FOPs across five supply chain partners.

Priority Capabilities Clusters:
These capability clusters have been prioritised because they directly address the most pressing challenges and opportunities in the process of **securing 'Tomorrow's Energy' by enabling sovereign digital security in critical national infrastructures (CNI)**

- **Cluster 1:** Sovereign cyber-security architectures for hybrid OT/IT energy systems.
- **Cluster 2:** AI-Enabled threat detection, surveillance and autonomous response.
- **Cluster 3:** Secure digitalisation of SCADA, IoT and edge Infrastructure.
- **Cluster 4:** Privacy-preserving data exchange and cryptographic security mechanisms.
- **Cluster 5**: Intelligent, secure supply chain and autonomous logistics ecosystems.

High-Priority FOPs:

The following roles will be instrumental in driving industry-wide change by facilitating informed decision-making and ensuring the compliance and economic viability of new technologies:

DevOps Engineer
IT Architects
IT Engineers
Power Systems Engineers
Security Controls and Instrumentation Manager

Education provision gaps:

One current apprenticeship, the High Integrity Software Engineer (ST0013), may be the scheme most affected of those available, due to the broad range of CNI competences and specialisations that it could facilitate. It is a four-year course at level six, with few others like it.

Priority capability themes

1. **Cyber security strategies for critical national infrastructure**
2. **SCADA system security and cloud migration**

3. **Advanced security protocols and frameworks**
4. **Optimisation and automation in energy sector**

Key Conclusions

A successful transition to a secure, net-zero energy system will depend on coordinated leadership within businesses and across the supply chain, accelerated workforce development, and structured collaboration between energy and cyber security sectors, as well as collaboration with educational institutions and regulators. While emerging technologies come across throughout the report as enablers for future business and societal objectives, they also introduce material risks, cost pressures, and capability gaps that are not currently addressed by existing workforce or educational provisions.

Risk and sustainability

There is the risk of positive feedback loops with the upskilling of workforces to accommodate emerging technologies, with a self-reinforcing cycle that increases the pressure to adopt further or faster as additional capabilities come online within a business.

Both quantum computing and AI/ML will impact sustainability governance practices, owing to the comparatively high environmental costs built into modern data centre infrastructure. They will similarly increase capital and operating expenditure, particularly in the following contexts:

- Secure infrastructure modernisation (cloud, edge, and hybrid environments)
- Cyber resilience and disaster recovery
- Regulatory compliance, monitoring, and assurance
- Workforce retraining and specialist CPD

At the same time, the report notes an increase in systemic risk, particularly as AI/ML expands in defensive and adversarial capabilities and similarly increases its own attack surfaces. Without adequate guardrails, this risk may extend into operational disruption, real-world harm, financial outlays, and reputational damage.

Leadership and collaboration

This cycle's findings point to a need for stronger cross-sector leadership. Responsibility for future readiness does not sit with a single organisation type but instead spans across several different types of supply-chain actors: energy operators, technology suppliers, SMEs, research bodies, educators, and regulators.

Collaboration is episodic and voluntary rather than systemic, and the cycle itself highlighted that workshops are effective in highlighting issues, but they are not themselves embedded into any clear, ongoing governance or planning process.

Leadership gaps may also become apparent in both the length of time needed for statutes to come into effect to regulate emerging technologies, and in the reliance on voluntary codes of practice to securely implement critical national infrastructure or services in the interim.

Workforce pressures

Current workforce provisions are insufficient for the anticipated changes across the horizon, at two to five years out. Even today, emerging technologies demonstrate increased capacity at much faster cadences than subject matter experts anticipated, both in terms of quantum computational performance and the ability of frontier AI models to surpass expectations in red team exercises. Against the 107 future capabilities identified, 66 have lack suitable matches within the existing apprenticeship standards and formal training routes.

The most acute gaps relate to:

- Advanced operational technology (OT) security
- Secure cloud migration of legacy SCADA systems
- AI/ML-enabled threat detection and response
- Privacy-preserving cryptographic techniques
- Secure, automated, and transparent supply chains

These gaps affect multiple roles, with DevOps Engineers, IT Architects, IT Engineers, Power Systems Engineers, and Security Controls specialists identified, on balance of probabilities, as being the most impacted. This cycle indicates that these roles will evolve rapidly and expand beyond the typical job definitions or descriptions used today.

Education framework

Achieving a secure net-zero energy system will require certain incremental changes to education and training provision. This includes:

- Updating curricula to reflect real-world CNI environments
- Expanding specialist CPD and modular learning pathways

The risk from emerging technologies, as documented in the report, underscores the need to align education more closely with regulatory and operational realities. This would be a more fundamental change, to formalise new skills and push them to the workforce at scale at faster cadences than existing frameworks for CPD allow. First and foremost, education is not as a downstream activity, but an enabling function that must evolve alongside both technology and policy.

CPD frameworks will be under pressure to become more adaptive and modular, with shorter turnaround times for the development of courses, reflecting the pace of change in both remote, cloud-based and cyber-physical (robotic) AI/ML products. Traditional qualification cycles have been described as too slow to respond.

State of the supply chain

There is a lack of continuous feedback between supply chain requirements, education provision, regulatory frameworks, and strategic national priorities. While supply chains are increasingly dependent and digitalised, the underlying frameworks and curricula remain largely siloed and subject only to incremental change. Regulatory expectations around data and code sovereignty, the resilience of critical national infrastructure, and the assurance or provenance of systems are all advancing faster than workforce capability alignment itself. This misalignment could hinder the pace of innovation and compliance.

Pace of change

Technology adoption will affect how work is done more generally, not merely the tools used. Some of the changes will include:

- A move from perimeter-based security to zero-trust and segmented architectures. Current-generation AI models have demonstrated an on-par ability with professional cyber security experts. Their ability to gain a foothold, chain exploits, and facilitate compromise point to a need for defence-in-depth and secure-by-design architectural models.
- A greater reliance on automated, AI-assisted monitoring and decision support. Blue team agents, comprising humans and AI/ML tools will become commonplace to ensure the speed of investigation and remediation matches the threat.

- An increased use of digital twins, testbeds, and simulation for assurance. Given the costs of implementing changes to infrastructure, the use of out-of-band evidence from digital twins will be necessary to support decision-making.
- A more explicit governance model for human–AI interaction and accountability. This should reflect the research conducted by government agencies and departments, particularly the AI Security Institute and NCSC.

These changes will be necessary for resilience, but they will also induce additional, new professional norms and oversight models.

Strategic priorities
Across the report, the following strategic priorities are consistent:

- Sovereign and resilient cyber security architectures for hybrid OT/IT systems
- Secure digitalisation and cloud migration of SCADA and operational assets
- AI-enabled threat detection with human oversight and assurance
- Privacy-preserving data exchange and cryptographic security
- Secure, transparent, and automated supply-chain operations

These priorities are framed as potentially mutually reinforcing rather than independent initiatives.

There is a clear emphasis on the need for new organisational guardrails and policies to reduce harms associated with emerging technologies, particularly where AI systems could influence operational safety functions and critical national infrastructure either directly or indirectly.

Summary
Novel AI/ML capabilities in the workforce are inevitable but neither sufficient nor obligatory for all businesses and stakeholders. Leadership, workforce investment, education reform, and clearly defined guardrails will serve to co-ordinate the emergence and development of these near-future occupational functions and capabilities in society. Without the necessary steering, however, the transition to a secure, net-zero energy future risks being slower, more costly, and less resilient than intended.

3.2 What this means for Industry

Insights from this cycle indicate important follow-on actions for industry to pursue next:

Invest in guardrail research and disaster recovery preparation
Explore what safety and security policies or guardrails would need to exist within the business, or wider industry, to reduce harm should AI/ML become widely integrated. Anticipate having a means to compartmentalise and protect controlled environments, high-value systems, business functions, and operations from the use of AI/ML regardless of whether its use is benign or malicious.

Collaborate with security institutions
Discuss the pitfalls and opportunities in AI/ML with UK stakeholders, notably the AI Security Institute and NCSC, and integrate their own reports in any data used to assess future, in-job training provisions.

Integrate sustainability into education processes

Anticipate financial, energy, and reputational costs from the use of emerging technologies and how they might conflict with implementing a net-zero economy. Consider adapting an environmental governance model to include AI/ML and other forms of non-traditional compute.

Upskill existing workforces
Examine how technical professionals can be retrained for existing business functions that stand to gain the most from upcoming emerging technologies, particularly AI/ML and quantum compute.

E**xpand current roles**
Evaluate how to bolster operational and engineering capabilities, to match pace with the on-going challenges presented by agent development and post-quantum cryptography and secure against the threats they present when used maliciously.

Reskill and borrow from other sectors
Assess where and how skills are being developed in tangential industries, and what could be appropriated to inform and improve knowledge within energy CNI and cyber security specifically.

3.3 What this means for Educators

Data collected from the workshops also highlights several opportunities and tasks worth pursuing by educators:

Adapt existing programmes
Review and revise existing and retired apprenticeships for the cyber security and energy sectors, to address the identified gaps in capability. Examples of retired schemes include **Power Engineer** (ST0153) and **Cyber Intrusion Analyst** (ST0114). Current schemes include the **High Integrity Software Engineer** (ST0013), **Cyber Security Technician** (ST0865), **Cyber Security Technologist** (ST1021), and **Cyber Security Technical Professional** (ST0409).

Develop flexible CPD courses
Design short courses that target specific future capabilities, to aid in retraining staff who wish to specialise or migrate from another sector.

Identify risk
Advise organisational leadership on the future implications for financing, monitoring, and regulating staff with access to more powerful AI resources available to them.

Prioritise technical development
Anticipate the potential future need for lab-based course material to debug, evaluate, and reprioritise AI agents. Provide training that current AI models lack data including held-out datasets, to push students to depend less on bots as oracles.

Collaborate with industry and regulators
Align educational priorities with the government's strategic objectives pertaining to cyber security and critical national infrastructure. Ensure that planned capabilities are likely to satisfy the upcoming requirements for the sectors to be ready for net-zero energy and discuss challenges, particularly the risk of an over-dependence on AI, with stakeholders in government.

Assess current qualification levels
Review the provision at present for critical national infrastructure training, particularly ST0013, and whether additional apprenticeship levels are necessary to complement it across more specific CNI sectors. Evaluate opportunities to work with independent training providers, and institutions in further and higher education.

Incorporate data and visualisations
Make use of the report's visualisation tool and the appendices to inform decision-making and planning around future curriculums.

Assess new techniques
Evaluate the usefulness of blue (defenders) and red (attackers) team exercises in the development of cyber security labs. Assess how to inform curriculum development using academic research around emergent technologies, particularly in AI/ML, SCADA hybridisation, and quantum computing.

3.4 Summary of next steps:

To ensure that the transition to net-zero can be done safely and securely, there are several actions to recommend at the close of this report:

Develop a technology roadmap
Use the feedback from technologists and industrial experts, as well as evidence from third parties, to plan what capabilities will be needed at which points in time over the horizon period, within the next two to five years. Anticipate which job functions and occupational profiles will change the most and the soonest.

Update CPD and apprenticeship standards
Stakeholders ought to collaborate in updating and reviewing cyber security apprenticeships and opportunities for CPD, especially where trainees demonstrate an interest in specialising in critical national infrastructure.

Ensure strategic alignment
Establish a procedure to monitor regulatory and statutory change, policy initiatives, and the strategic ambitions of the UK Government, to help align training provision and the direction of travel across the public sector. Examples of recent policy papers and bills include the following:

- Cyber Security and Resilience Bill (Department for Science, 2024)
- Government Cyber Security Strategy: 2022 to 2030 (Cabinet Office, 2026)
- Overarching National Policy Statement for energy (EN-1) (HM Government, 2026)
- UK Infrastructure: A 10 Year Strategy (HM Tresaury and National Infrastructure and Service Transformation Authority, 2025)

Evaluate overseas training practices
Similar training provisions may be further developed in other EU countries or in the Americas, hence it would be expedient to evaluate the state of the art in technology education and upskilling abroad. Use any matching overseas training provisions, whether in AI/ML, quantum computing, or robotics, as evidence to support the case for greater investment in the UK, within energy CNI and cyber security.

Assess knowledge sharing opportunities

Investigate how partner industries, universities, and innovation agencies domestically and overseas have tackled the changes of net-zero and infrastructure sovereignty and whether they may be untapped opportunities to share knowledge and learn.

Engage additional stakeholders
To further disseminate findings, either at higher levels within the public sector or CNI supply chains, reach out to local, sitting Members of Parliament, Select Committees, and industrial associations. Share evidence and discuss how to develop momentum for new cyber security practices and skills in industry.

Schedule complementary workshops
Given the UK's national priorities and the overall pace of technological change, new workshops should be pursued at regular cadences to help routinely identify upcoming shortfalls and any current gaps in workforce knowledge.

References

Cabinet Office, 2026. *Government Cyber Security Strategy: 2022 to 2030*. [Online]
Available at: https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030

Department for Business and Trade, 2025. *The UK's Modern Industrial Strategy 2025*. [Online]
Available at: https://www.gov.uk/government/collections/the-uks-modern-industrial-strategy-2025

Department for Energy Security and Net Zero, 2025. *UK ENERGY IN BRIEF 2025*. [Online]
Available at:
https://assets.publishing.service.gov.uk/media/688890c3a11f859994409132/UK_Energy_in_Brief_2025.pdf

Department for Science, Innovation and Technology, 2025. *Cyber security sectoral analysis 2025*. [Online].

Department for Science, I. a. T., 2024. *Cyber Security and Resilience Bill*. [Online]
Available at: https://www.gov.uk/government/collections/cyber-security-and-resilience-bill

HM Government, 2026. *Overarching National Policy Statement for energy (EN-1), 2025*. [Online]
Available at: https://www.gov.uk/government/publications/overarching-national-policy-statement-for-energy-en-1-2025/overarching-national-policy-statement-for-energy-en-1-2025-accessible-webpage

HM Tresaury and National Infrastructure and Service Transformation Authority, 2025. *UK Infrastructure: A 10 Year Strategy*. [Online]
Available at: https://www.gov.uk/government/publications/uk-infrastructure-a-10-year-strategy

Appendix

Appendix

Appendix A Online Data visualisation tool

The interested reader may wish to access the online data visualisation tool which provides several different ways to view the cycle data. Links to relevant parts of the tool are given with brief guidance below. This content is provided and maintained by the Workforce Foresighting Hub.

Visualisation tool section	What is it and what can it be used for?
Data Capture Overview	Provides a summary of the data captured across the foresight cycle, bringing together the work of the Technologists / Domain Specialists, Employers and Educators into one overview. Full URL:: https://hvmcatapultforesighting.retool.com/embedded/public/e869283b-4b8a-437c-973e-64ab292e5b87?token=5a8879cd93ad5f696919b4149f544e96
Supply Chain Capabilities	Provides an overview of the identified capabilities at a Supply Chain / Workflow Partner level. By selecting/deselecting each Supply Chain / Workflow Partner you can review the capabilities identified as required in that area of the Supply Chain / Workflow. This can be used to generate organisational capability profiles for each area of the workflow /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. Full URL: https://hvmcatapultforesighting.retool.com/embedded/public/3573002a-ab48-4fad-9765-bee00876a42e?token=5a8879cd93ad5f696919b4149f544e96
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 Family 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. Full URL: https://hvmcatapultforesighting.retool.com/embedded/public/81d272f0-ad80-421c-8926-86655913acdf?token=5a8879cd93ad5f696919b4149f544e96

Visualisation tool section	What is it and what can it be used for?
FOP Matrix	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 family by selecting one (or more) of these from the drop down. This will then allow you to select the FOPs aligned to that role family. The populated table allows you review and compares different FOPs within or across role families. You can view the capabilities in each FOP and the assigned proficiency levels. You can also toggle 'Hide Empty Capabilities' on/off to reduce the view down to only those capabilities included in the role family you are reviewing. Full URL: https://hvmcatapultforesighting.retool.com/embedded/public/f99a913f-8827-4730-8893-d618d489bc84?token=5a8879cd93ad5f696919b4149f544e96
Future KSBs Summary	Not yet completed in this cycle. 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 family/occupational profile grouping. Full URL: https://hvmcatapultforesighting.retool.com/embedded/public/8634650f-9700-4627-8431-068b4b764222?token=5a8879cd93ad5f696919b4149f544e96

Visualisation tool section	What is it and what can it be used for?
FOP Distribution	This page allows provides a breakdown of the Capabilities within the selected Cycle and how they are distributed across the FOPs with the addition of a distribution chart showing the required proficiency across those FOPs. Clicking the “View FOPs” button alongside each capability will provide a list of the proficiencies (EPA) with the FOPs that fall into them. The exported version of this data will include a full breakdown of the FOP IDs which contain the capability within a specific proficiency. This is used to: • understand the levels/volumes of common/crossover Capabilities, to support prioritisation of Capability Development • identify which Occupational Profiles contain these common/crossover capabilities, and so which may be prioritised for development activity Full URL: https://hvmcatapultforesighting.retool.com/embedded/public/ce67cca1-5beb-4557-8482-8a0b6e174933?token=5a8879cd93ad5f696919b4149f544e96
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 (Skills England Occupational Standards) provision. • By capabilities that are not served by the reference mapping framework, e.g., Skills England Occupational Standards 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 Occupational 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. Full URL: https://hvmcatapultforesighting.retool.com/embedded/public/219ff6af-36ea-4b5e-bda1-b0b989c0e3f0?token=5a8879cd93ad5f696919b4149f544e96

Visualisation tool section	What is it and what can it be used for?
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 (Skills England Occupational Standards). 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. Full URL https://hvmcatapultforesighting.retool.com/embedded/public/c699e504-3f64-45a0-b52e-ad44a95f9aa4?token=5a8879cd93ad5f696919b4149f544e96
Fit & Surplus Matrix	This page is a visual representation of the 'Fit and Surplus Factor' insight. You can visually review 'Fit' and 'Surplus' of Future Occupation Profiles (FOP) against existing training provision e.g. Institute for Apprenticeships and Technical Education (Skills England Occupational Standards). 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. Full URL: https://hvmcatapultforesighting.retool.com/embedded/public/1c4e204b-3927-4226-9f8e-2f62ce0643c5?token=5a8879cd93ad5f696919b4149f544e96
FOP Capability Matches	This page allows you to view the matches between Capabilities and Institute for Apprenticeships and Technical Education (Skills England Occupational Standards) 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 FOPs or review all FOPs under a Role Family, to give a more holistic view of Capabilities and Matches Where a future capability has been matched to existing provision (currently, by default, Skills England Occupational 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 Families and FOPs, from Job / Occupation level through to Knowledge, Skill and Behaviour level Full URL https://hvmcatapultforesighting.retool.com/embedded/public/6a205e7e-8f33-4765-b39b-82f1f549217a?token=5a8879cd93ad5f696919b4149f544e96

Visualisation tool section	What is it and what can it be used for?
FOP vs Provision	This page allows you to compare FOPs against existing Skills England Occupational Standards. The information here allows you to prioritise effort or action over the short, medium or long-term. This is displayed as a Matched/Not Matched Capability, comparing the Capability in a FOP to the Duties in a Standard. The left-hand side allows you to select the Role Family and FOP, while the right-hand modal allows you to compare against the top 10 matched Skills England Occupational Standards for that Occupational Profile. Where a future capability has been matched to existing provision (currently, by default, Skills England Occupational 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. Full URL: https://hvmcatapultforesighting.retool.com/embedded/public/d9f485a2-6d23-45dd-ab48-4c4c87ced0c7?token=5a8879cd93ad5f696919b4149f544e96:
FOP Priorities	Provides a list of all the FOPs within the selected cycle with details of their fit and surplus factors. The information here allows you to prioritise effort or action over the short, medium or long-term. Full URL https://hvmcatapultforesighting.retool.com/embedded/public/ad0f6dcb-9535-4239-96a7-c8d0e005477a?token=5a8879cd93ad5f696919b4149f544e96:

Table 17: Online Data visualisation tool

Appendix B Capabilities not served (unmatched) by Skills England provision

The full 66 unmatched capabilities indicating their relevant supply chain partners

Supply chain partner table key:

1. RTO/COI - Research & Innovation Organisations
2. Original Equipment Manufacturers (OEM's), Primes, Tier-1s
3. Small to Medium Enterprises (SMEs)
4. Equipment Service Providers
5. Regulatory Organisations

Function Area	Capability Statement	1	2	3	4	5
SUPPORT	Develop interoperable data standards to facilitate seamless and secure cross-organisational data sharing.	✓	✓	✓	✓	✓
SUPPORT	Establish interoperability frameworks to ensure seamless integration of diverse security protocols across systems.	✓	✓	✓	✓	✓
SUPPORT	Develop and enforce security-by-design principles to ensure IoT devices meet regulatory standards.	✓	✓	✓	✓	✓
SUPPORT	Develop SCADA migration strategies to ensure secure and efficient transition to cloud environments.	✓	✓	✓	✓	
SUPPORT	Integrate AI-enhanced anomaly detection to monitor and secure critical infrastructure systems against potential disruptions.	✓	✓	✓	✓	
SUPPORT	Design secure network architectures for critical infrastructure to prevent unauthorized access and ensure system resilience.	✓	✓	✓	✓	
SUPPORT	Utilize tamper-proof AI models to maintain the integrity and availability of critical national infrastructure systems.	✓	✓	✓	✓	
SUPPORT	Implement network segmentation to isolate SCADA systems from corporate IT networks and enhance security.		✓	✓	✓	
SUPPORT	Integrate AI-driven surveillance systems to enhance real-time threat detection and response in critical national infrastructure facilities.	✓	✓	✓	✓	
SUPPORT	Develop interoperability frameworks to integrate legacy systems with modern digital security protocols.	✓	✓	✓	✓	✓
SUPPORT	Implement zero trust architectures to enhance security across critical national infrastructures.	✓	✓	✓	✓	✓
SUPPORT	Implement sovereign digital platforms to secure AI and cloud infrastructures within national borders.	✓	✓	✓	✓	
SUPPORT	Integrate MCP with existing security frameworks to strengthen resilience against cyber threats in energy sector infrastructures.	✓	✓	✓	✓	✓
SUPPORT	Conduct vulnerability assessments on MCP implementations to identify and mitigate potential security risks in critical systems.	✓	✓	✓	✓	
SUPPORT	Deploy a tailored AI-driven customer support system that utilizes chatbots and voice assistants to enhance user interaction and support.			✓	✓	✓

Function Area	Capability Statement	1	2	3	4	5
ENTERPRISE	Integrate artificial intelligence-driven threat detection systems to proactively identify and mitigate cyber threats in critical national infrastructures.	✓	✓	✓	✓	
ENTERPRISE	Implement AI-driven anomaly detection to identify and mitigate cyber threats in critical national infrastructure.	✓	✓	✓	✓	
ENTERPRISE	Analyse and identify specific threats to major security systems to enhance protection measures.	✓	✓	✓	✓	
ENTERPRISE	Encrypt data in transit and at rest to protect sensitive information within IoT networks.	✓	✓	✓	✓	✓
ENTERPRISE	Conduct regular vulnerability assessments to identify and mitigate risks within energy data management systems.	✓	✓	✓	✓	
ENTERPRISE	Utilize edge computing to process data locally, reducing latency and enhancing security in IoT deployments.	✓	✓	✓	✓	
ENTERPRISE	Implement secure data-sharing protocols to facilitate confidential information exchange between energy sector organisations.	✓	✓	✓	✓	✓
ENTERPRISE	Implement secure data exchange protocols to facilitate safe and efficient cross-organisation data sharing.	✓	✓	✓	✓	✓
ENTERPRISE	Establish sovereign cloud environments to ensure data sovereignty and compliance with national security regulations in critical infrastructure sectors.	✓	✓	✓	✓	✓
ENTERPRISE	Implement secure data-sharing protocols within dashboards to ensure compliance with national cybersecurity regulations for critical national infrastructure.	✓	✓	✓	✓	✓
ENTERPRISE	Implement zero-knowledge proof protocols to verify system integrity without exposing sensitive data.	✓	✓	✓	✓	
ENTERPRISE	Develop secure MCP client-server architectures to enhance data integrity and confidentiality in critical national infrastructures.	✓	✓	✓	✓	
ENTERPRISE	Develop secure communication protocols to protect data transmission within critical national infrastructure systems.	✓	✓	✓	✓	✓
ENTERPRISE	Establish secure communication protocols to protect data transmission within critical national infrastructure systems.	✓	✓	✓	✓	✓
ENTERPRISE	Develop software (and AI) tools for detecting and preventing security threats.	✓	✓	✓	✓	
ENTERPRISE	Monitor cloud-based control system integrations to ensure they meet UK national cybersecurity standards for critical infrastructures.	✓	✓	✓	✓	✓
ENTERPRISE	Monitor cyber security compliance to ensure adherence to relevant standards.		✓	✓	✓	✓
DESIGN	Develop AI-driven threat detection algorithms to identify and mitigate cyber threats in critical national infrastructure systems.	✓	✓	✓	✓	
DESIGN	Develop and deploy smart contracts to automate and enforce agreements within critical national infrastructures.	✓	✓	✓		
DESIGN	Develop and implement zero-knowledge proof protocols for specific critical national infrastructure systems to	✓	✓	✓		

Function Area	Capability Statement	1	2	3	4	5
	improve data privacy and ensure robust security measures.					
DESIGN	Develop analytics tools for monitoring and analysing specific critical infrastructure networks to enhance their security and performance.	✓	✓	✓	✓	
DESIGN	Develop zero-trust architectures for critical national infrastructures to enhance cybersecurity resilience.	✓	✓	✓	✓	✓
DESIGN	Develop hardware solutions with industry partners to enhance security for critical national infrastructure, specifically by implementing Trusted Execution Environment technologies.		✓	✓	✓	
DESIGN	Integrate digital twin technologies with energy infrastructures to enhance resilience against cyber threats.	✓	✓	✓	✓	
DESIGN	Develop interfaces for teaming between humans and AI, focusing on explicit transfer points and authority for decisions, streamlining process efficiency and accountability	✓	✓	✓	✓	
DESIGN	Design governance mechanisms for AI-enabled systems to ensure auditability and decision accountability.	✓	✓	✓	✓	✓
DESIGN	Design processes for system prototypes to test AI failure scenarios to optimise and improve system reliability	✓	✓	✓	✓	
DESIGN	Develop AI-driven threat detection algorithms to identify and mitigate cyber threats in critical national infrastructure systems.	✓	✓	✓	✓	
DESIGN	Develop and deploy smart contracts to automate and enforce agreements within critical national infrastructures.	✓	✓	✓		
DESIGN	Develop and implement zero-knowledge proof protocols for specific critical national infrastructure systems to improve data privacy and ensure robust security measures.	✓	✓	✓		
DESIGN	Develop analytics tools for monitoring and analysing specific critical infrastructure networks to enhance their security and performance.	✓	✓	✓	✓	
DESIGN	Develop zero-trust architectures for critical national infrastructures to enhance cybersecurity resilience.	✓	✓	✓	✓	✓
DESIGN	Develop hardware solutions with industry partners to enhance security for critical national infrastructure, specifically by implementing Trusted Execution Environment technologies.		✓	✓	✓	
DESIGN	Integrate digital twin technologies with energy infrastructures to enhance resilience against cyber threats.	✓	✓	✓	✓	
DESIGN	Develop interfaces for teaming between humans and AI, focusing on explicit transfer points and authority for decisions, streamlining process efficiency and accountability	✓	✓	✓	✓	
DESIGN	Design governance mechanisms for AI-enabled systems to ensure auditability and decision accountability.	✓	✓	✓	✓	✓
DESIGN	Design processes for system prototypes to test AI failure scenarios to optimise and improve system reliability	✓	✓	✓	✓	

Function Area	Capability Statement	1	2	3	4	5
DESIGN	Develop interoperability frameworks for critical national infrastructure to ensure secure data exchange between different systems.		✓			
DESIGN	Design interfaces to define clear roles and decision points between human staff, robots, and AI systems to enhance procedural efficiency and accountability.		✓			
IMPLEMENT	Establish secure testbeds for SCADA migration to validate system performance and security before deployment.		✓	✓	✓	
IMPLEMENT	Develop SCADA migration utilities to facilitate seamless transition from legacy systems to modern platforms.		✓	✓	✓	
IMPLEMENT	Develop and implement network segmentation strategies to isolate operational technology systems from information technology networks, enhancing security and reducing attack surfaces.		✓	✓	✓	
IMPLEMENT	Operate SCADA systems securely and resiliently in the cloud to enhance critical infrastructure operations and data accessibility.		✓	✓	✓	
IMPLEMENT	Design security controllers for critical national infrastructure SCADA systems to improve specific operational metrics and guarantee consistent system performance.		✓	✓	✓	
IMPLEMENT	Implement critical national infrastructure grade SCADA-in-the-cloud specific security solutions to enhance operational efficiency and scalability.		✓	✓	✓	
IMPLEMENT	Develop integration solutions between multiple cloud platforms and original equipment manufacturers to enhance system resilience and data accessibility.		✓	✓	✓	
IMPLEMENT	Develop niche AI analytics tools to analyse and interpret complex data patterns within critical national infrastructure networks.		✓	✓	✓	
IMPLEMENT	Install AI monitoring tools to continuously oversee and assess the security posture of critical national infrastructure components.		✓	✓	✓	
IMPLEMENT	Using advanced computational modelling techniques to optimize energy generation processes.		✓	✓		
IMPLEMENT	Develop edge AI solutions to enable on-device data processing for improved security and efficiency in energy systems.		✓	✓	✓	
IMPLEMENT	Analyse facility energy demands and generation constraints to maximise the efficient utilisation of low carbon energy sources in specific operational sectors.		✓	✓		
LOGISTICS	Demonstrate the application of zero-knowledge protocols within ERP and logistics planning solutions	✓				
LOGISTICS	Demonstrate AI solution effectiveness in assessing product quality control compliance.	✓				
LOGISTICS	Adopt specific autonomous transport protocols to enhance logistic precision and warehouse operations efficiency.		✓			
LOGISTICS	Integrate AI solutions into the software used for checking product availability to enhance logistics processes.		✓	✓	✓	
LOGISTICS	Integrate zero-knowledge protocols with enterprise resource planning systems to enhance security for logistics planning solutions.			✓	✓	

Function Area	Capability Statement	1	2	3	4	5
LOGISTICS	Operate secure-by-design integration, delivery, and maintenance chains to ensure consistent system reliability and security compliance.		✓			
LOGISTICS	Create a verifiable bill of materials for hardware and software components to ensure accurate tracking and maintenance.		✓	✓	✓	
LOGISTICS	Design and validate automation suites to optimise, rationalise, and adopt component procurement strategies				✓	
LOGISTICS	Integrate automation suites to optimise, rationalise, and adopt component procurement strategies				✓	
LOGISTICS	Adopt AI solutions in the assessment of quality controls compliance for products			✓	✓	

Table 18: B1 Capabilities not served(unmatched) by Skills England provision

Appendix C List of full Future Occupational Profiles

FOP Title IT Information Managers
Role Level Strategic & Operational Management
Required for supply chain partners Original Equipment Manufacturers (OEM's), Primes, Tier-1s; Small to Medium Enterprises (SMEs); RTO/COI - Research & Innovation Organisations; Equipment Service Providers; Regulatory Organisations

ID	Capability Statement	Proficiency
322343	Integrate MCP with existing security frameworks to strengthen resilience against cyber threats in energy sector infrastructures.	**Awareness**
322265	Integrate AI-driven surveillance systems to enhance real-time threat detection and response in critical national infrastructure facilities.	**Awareness**
322199	Implement network segmentation to isolate SCADA systems from corporate IT networks and enhance security.	**Awareness**
322824	Use AI generated interactive content to facilitate learning and training in safety standards	**Awareness**
322822	Use AI generated interactive content to facilitate specialised training in complex environments	**Awareness**
322807	Utilise AI-based forensic analysis to investigate and respond to cyber incidents affecting critical infrastructure.	**Awareness**
322043	Integrate artificial intelligence-driven threat detection systems to proactively identify and mitigate cyber threats in critical national infrastructures.	**Awareness**
322825	Deploy a tailored AI-driven customer support system that utilizes chatbots and voice assistants to enhance user interaction and support.	**Awareness**
323112	Develop interoperability frameworks for critical national infrastructure to ensure secure data exchange between different systems.	**Expert**
312602	Monitor cyber security compliance to ensure adherence to relevant standards.	**Expert**
322812	Monitor cloud-based control system integrations to ensure they meet UK national cybersecurity standards for critical infrastructures.	**Expert**
322178	Implement secure data-sharing protocols to facilitate confidential information exchange between energy sector organisations.	**Expert**
322157	Conduct regular vulnerability assessments to identify and mitigate risks within energy data management systems.	**Expert**
322809	Establish secure communication protocols to protect data transmission within critical national infrastructure systems.	**Expert**
322808	Develop secure communication protocols to protect data transmission within critical national infrastructure systems.	**Expert**
322230	Implement secure data exchange protocols to facilitate safe and efficient cross-organisation data sharing.	**Expert**
322080	Develop interoperable data standards to facilitate seamless and secure cross-organisational data sharing.	**Expert**

321697	Ensure security by design in all system development processes to protect against cyber and physical threats.	**Expert**
322277	Implement secure data-sharing protocols within dashboards to ensure compliance with national cybersecurity regulations for critical national infrastructure.	**Expert**
322801	Establish digital identities and access control protocols for devices, users, and systems across energy networks to ensure secure and verifiable interactions.	**Expert**
322270	Develop interoperability frameworks to integrate legacy systems with modern digital security protocols.	**Expert**
322244	Establish sovereign cloud environments to ensure data sovereignty and compliance with national security regulations in critical infrastructure sectors.	**Expert**
322118	Establish interoperability frameworks to ensure seamless integration of diverse security protocols across systems.	**Expert**
322271	Implement zero trust architectures to enhance security across critical national infrastructures.	**Expert**
322287	Implement sovereign digital platforms to secure AI and cloud infrastructures within national borders.	**Expert**

Table 19: IT Information Managers FOP

FOP Title Managers in Logistics
Role Level Strategic & Operational Management
Required for supply chain partners Original Equipment Manufacturers (OEM's), Primes, Tier-1s; Small to Medium Enterprises (SMEs); Equipment Service Providers.

ID	Capability Statement	Proficiency
322822	Use AI generated interactive content to facilitate specialised training in complex environments	**Awareness**
322824	Use AI generated interactive content to facilitate learning and training in safety standards	**Awareness**
323126	Develop decision models that integrate secured logistics data to ensure reliable delivery of infrastructure components and parts to partners.	**Expert**
323118	Adopt specific autonomous transport protocols to enhance logistic precision and warehouse operations efficiency.	**Expert**
323121	Integrate AI solutions into the software used for checking product availability to enhance logistics processes.	**Expert**

Table 20: Managers in Logistics FOP

FOP Title Lifecycle Risk Managers
Role Level Strategic & Operational Management
Required for supply chain partners Original Equipment Manufacturers (OEM's), Primes, Tier-1s; Small to Medium Enterprises (SMEs); RTO/COI - Research & Innovation Organisations; Equipment Service Providers; Regulatory Organisations

ID	Capability Statement	Proficiency
322811	Conduct cybersecurity risk assessments to identify vulnerabilities and enhance resilience in critical energy infrastructure.	**Expert**
322157	Conduct regular vulnerability assessments to identify and mitigate risks within energy data management systems.	**Expert**
322344	Conduct vulnerability assessments on MCP implementations to identify and mitigate potential security risks in critical systems.	**Expert**
322813	Integrate fraud detection systems into digital transaction platforms to enhance security and monitor for fraudulent activities.	**Expert**
322821	Implement measures to ensure the secure use of AI in new or existing software lifecycle management processes	**Expert**

323110	Demonstrate the added value from automation suites that can rationalise business procurement strategies	Expert
322277	Implement secure data-sharing protocols within dashboards to ensure compliance with national cybersecurity regulations for critical national infrastructure.	Expert

Table 21: Lifecycle Risk Managers FOP

FOP Title Compliance and Regulatory Professionals
Role Level Professional and Delivery
Required for supply chain partners Original Equipment Manufacturers (OEM's), Primes, Tier-1s; Small to Medium Enterprises (SMEs); RTO/COI - Research & Innovation Organisations; Equipment Service Providers; Regulatory Organisations

ID	Capability Statement	Proficiency
312602	Monitor cyber security compliance to ensure adherence to relevant standards.	Expert
322251	Develop and enforce security-by-design principles to ensure IoT devices meet regulatory standards.	Expert
323123	Adopt AI solutions in the assessment of quality controls compliance for products	Expert
323119	Operate secure-by-design integration, delivery, and maintenance chains to ensure consistent system reliability and security compliance.	Expert
322244	Establish sovereign cloud environments to ensure data sovereignty and compliance with national security regulations in critical infrastructure sectors.	Expert
322277	Implement secure data-sharing protocols within dashboards to ensure compliance with national cybersecurity regulations for critical national infrastructure.	Expert
322812	Monitor cloud-based control system integrations to ensure they meet UK national cybersecurity standards for critical infrastructures.	Expert
323103	Provide training to engage with national and international standards development organisations (SDO)	Expert
322344	Conduct vulnerability assessments on MCP implementations to identify and mitigate potential security risks in critical systems.	Expert
322080	Develop interoperable data standards to facilitate seamless and secure cross-organisational data sharing.	Expert
322819	Design governance mechanisms for AI-enabled systems to ensure auditability and decision accountability.	Expert
322118	Establish interoperability frameworks to ensure seamless integration of diverse security protocols across systems.	Expert
322230	Implement secure data exchange protocols to facilitate safe and efficient cross-organisation data sharing.	Expert

323130	Implement chain of custody procedures to ensure secure handling of hardware and deploy calibration procedures to maintain accuracy in measurements.	**Expert**
322277	Implement secure data-sharing protocols within dashboards to ensure compliance with national cybersecurity regulations for critical national infrastructure.	**Expert**
322812	Monitor cloud-based control system integrations to ensure they meet UK national cybersecurity standards for critical infrastructures.	**Expert**
323103	Provide training to engage with national and international standards development organisations (SDO)	**Expert**
322344	Conduct vulnerability assessments on MCP implementations to identify and mitigate potential security risks in critical systems.	**Expert**

Table 22: Compliance and Regulatory Professionals FOP

FOP Title DevOps Engineers
Role Level Professional and Delivery
Required for supply chain partners Original Equipment Manufacturers (OEM's), Primes, Tier-1s; Small to Medium Enterprises (SMEs); RTO/COI - Research & Innovation Organisations; Equipment Service Providers; Regulatory Organisations

ID	Capability Statement	Proficiency
312602	Monitor cyber security compliance to ensure adherence to relevant standards.	Expert
322251	Develop and enforce security-by-design principles to ensure IoT devices meet regulatory standards.	Expert
323123	Adopt AI solutions in the assessment of quality controls compliance for products	Expert
323119	Operate secure-by-design integration, delivery, and maintenance chains to ensure consistent system reliability and security compliance.	Expert
322244	Establish sovereign cloud environments to ensure data sovereignty and compliance with national security regulations in critical infrastructure sectors.	Expert
322277	Implement secure data-sharing protocols within dashboards to ensure compliance with national cybersecurity regulations for critical national infrastructure.	Expert
322812	Monitor cloud-based control system integrations to ensure they meet UK national cybersecurity standards for critical infrastructures.	Expert
323103	Provide training to engage with national and international standards development organisations (SDO)	Expert
322344	Conduct vulnerability assessments on MCP implementations to identify and mitigate potential security risks in critical systems.	Expert
322080	Develop interoperable data standards to facilitate seamless and secure cross-organisational data sharing.	Expert
322819	Design governance mechanisms for AI-enabled systems to ensure auditability and decision accountability.	Expert
322118	Establish interoperability frameworks to ensure seamless integration of diverse security protocols across systems.	Expert
322230	Implement secure data exchange protocols to facilitate safe and efficient cross-organisation data sharing.	Expert
323130	Implement chain of custody procedures to ensure secure handling of hardware and deploy calibration procedures to maintain accuracy in measurements.	Expert
322277	Implement secure data-sharing protocols within dashboards to ensure compliance with national cybersecurity regulations for critical national infrastructure.	Expert
322812	Monitor cloud-based control system integrations to ensure they meet UK national cybersecurity standards for critical infrastructures.	Expert

Table 23: DevOps Engineers FOP

FOP Title IT Architects
Role Level Professional and Delivery
Required for supply chain partners Original Equipment Manufacturers (OEM's), Primes, Tier-1s; Small to Medium Enterprises (SMEs); RTO/COI - Research & Innovation Organisations; Equipment Service Providers; Regulatory Organisations

ID	Capability Statement - IT Architects	Proficiency
323124	Integrate zero-knowledge protocols with enterprise resource planning systems to enhance security for logistics planning solutions.	**Awareness**
322177	Utilize tamper-proof AI models to maintain the integrity and availability of critical national infrastructure systems.	**Awareness**
322199	Implement network segmentation to isolate SCADA systems from corporate IT networks and enhance security.	**Awareness**
213828	Support transport networking infrastructure and digital engineering designs to optimise overall network performance.	**Awareness**
322802	Integrate tamper-resistant transaction and audit mechanisms to support secure energy markets and fraud detection.	**Awareness**
323125	Design and validate zero-knowledge protocols within ERP and logistics planning solutions	**Practitioner**
322046	Develop SCADA migration strategies to ensure secure and efficient transition to cloud environments.	**Expert**
322805	Design secure cloud platforms to support scalable and resilient energy management services.	**Expert**
322816	Develop integration solutions between multiple cloud platforms and original equipment manufacturers to enhance system resilience and data accessibility.	**Expert**
322230	Implement secure data exchange protocols to facilitate safe and efficient cross-organisation data sharing.	**Expert**
323112	Develop interoperability frameworks for critical national infrastructure to ensure secure data exchange between different systems.	**Expert**
322341	Develop secure MCP client-server architectures to enhance data integrity and confidentiality in critical national infrastructures.	**Expert**
322790	Develop zero-trust architectures for critical national infrastructures to enhance cybersecurity resilience.	**Expert**
322330	Develop tamper-proof AI systems to maintain data integrity and prevent unauthorized modifications in critical infrastructures.	**Expert**
322244	Establish sovereign cloud environments to ensure data sovereignty and compliance with national security regulations in critical infrastructure sectors.	**Expert**
321697	Ensure security by design in all system development processes to protect against cyber and physical threats.	**Expert**
322271	Implement zero trust architectures to enhance security across critical national infrastructures.	**Expert**
322277	Implement secure data-sharing protocols within dashboards to ensure compliance with national cybersecurity regulations for critical national infrastructure.	**Expert**
322814	Design security interfaces and decision-support tools to enable rapid, safe, and informed actions by critical national infrastructure activities.	**Expert**

ID	Capability Statement - IT Architects	Proficiency
323119	Operate secure-by-design integration, delivery, and maintenance chains to ensure consistent system reliability and security compliance.	Expert
322270	Develop interoperability frameworks to integrate legacy systems with modern digital security protocols.	Expert
322819	Design governance mechanisms for AI-enabled systems to ensure auditability and decision accountability.	Expert
323132	Implement secure automated pipelines for onboarding specialised cyber-physical systems, with mechanisms to effect different rollback strategies.	Expert
322808	Develop secure communication protocols to protect data transmission within critical national infrastructure systems.	Expert
322178	Implement secure data-sharing protocols to facilitate confidential information exchange between energy sector organisations.	Expert
322287	Implement sovereign digital platforms to secure AI and cloud infrastructures within national borders.	Expert
322804	Establish verifiable, tamper-resistant digital identities to ensure the security and traceability of critical infrastructure assets and data.	Expert
323126	Develop decision models that integrate secured logistics data to ensure reliable delivery of infrastructure components and parts to partners.	Expert
322080	Develop interoperable data standards to facilitate seamless and secure cross-organisational data sharing.	Expert
322293	Establish zero trust architectures to ensure secure communication and access control within IoT-enabled energy networks.	Expert
322788	Develop and implement zero-knowledge proof protocols for specific critical national infrastructure systems to improve data privacy and ensure robust security measures.	Expert
323120	Create a verifiable bill of materials for hardware and software components to ensure accurate tracking and maintenance.	Expert
321697	Ensure security by design in all system development processes to protect against cyber and physical threats.	Expert
322271	Implement zero trust architectures to enhance security across critical national infrastructures.	Expert
322277	Implement secure data-sharing protocols within dashboards to ensure compliance with national cybersecurity regulations for critical national infrastructure.	Expert
322814	Design security interfaces and decision-support tools to enable rapid, safe, and informed actions by critical national infrastructure activities.	Expert
323119	Operate secure-by-design integration, delivery, and maintenance chains to ensure consistent system reliability and security compliance.	Expert
322270	Develop interoperability frameworks to integrate legacy systems with modern digital security protocols.	Expert
322819	Design governance mechanisms for AI-enabled systems to ensure auditability and decision accountability.	Expert

Table 24: IT Architects FOP

FOP Title IT Engineers
Role Level Professional and Delivery
Required for supply chain partners Original Equipment Manufacturers (OEM's), Primes, Tier-1s; Small to Medium Enterprises (SMEs); RTO/COI - Research & Innovation Organisations; Equipment Service Providers; Regulatory Organisations

ID	**Capability Statement -** IT Engineers	Proficiency
322177	Utilize tamper-proof AI models to maintain the integrity and availability of critical national infrastructure systems.	**Awareness**
322802	Integrate tamper-resistant transaction and audit mechanisms to support secure energy markets and fraud detection.	**Awareness**
323106	Demonstrate the application of zero-knowledge protocols within ERP and logistics planning solutions	**Awareness**
322794	Develop advanced cryptographic authentication mechanisms to securely bind digital twins to their corresponding physical assets.	**Awareness**
323127	Integrate automation suites to optimise, rationalise, and adopt component procurement strategies	**Awareness**
322340	Utilise zero-knowledge proofs to enable secure, anonymous reporting systems in critical infrastructure networks.	**Awareness**
323122	Design AI solutions to improve parts and components availability in circuit design software.	**Awareness**
322816	Develop integration solutions between multiple cloud platforms and original equipment manufacturers to enhance system resilience and data accessibility.	**Expert**
322263	Develop niche AI analytics tools to analyse and interpret complex data patterns within critical national infrastructure networks.	**Expert**
323126	Develop decision models that integrate secured logistics data to ensure reliable delivery of infrastructure components and parts to partners.	**Expert**
322789	Develop analytics tools for monitoring and analysing specific critical infrastructure networks to enhance their security and performance.	**Expert**
322805	Design secure cloud platforms to support scalable and resilient energy management services.	**Expert**
322810	Develop software (and AI) tools for detecting and preventing security threats.	**Expert**
322292	Develop edge AI solutions to enable on-device data processing for improved security and efficiency in energy systems.	**Expert**
322149	Integrate edge computing solutions to enhance real-time data processing and operational efficiency in energy systems.	**Expert**
322080	Develop interoperable data standards to facilitate seamless and secure cross-organisational data sharing.	**Expert**
322065	Deploy AI-based predictive maintenance systems to proactively identify and address vulnerabilities in critical infrastructure components.	**Expert**
322793	Develop hybrid SCADA prototypes to validate interoperability between cloud-based services and existing operational technology systems.	**Expert**
322157	Conduct regular vulnerability assessments to identify and mitigate risks within energy data management systems.	**Expert**

ID	**Capability Statement -** IT Engineers	Proficiency
323121	Integrate AI solutions into the software used for checking product availability to enhance logistics processes.	**Expert**
323119	Operate secure-by-design integration, delivery, and maintenance chains to ensure consistent system reliability and security compliance.	**Expert**
322230	Implement secure data exchange protocols to facilitate safe and efficient cross-organisation data sharing.	**Expert**
323112	Develop interoperability frameworks for critical national infrastructure to ensure secure data exchange between different systems.	**Expert**
323132	Implement secure automated pipelines for onboarding specialised cyber-physical systems, with mechanisms to effect different rollback strategies.	**Expert**
322141	Integrate AI-enhanced anomaly detection to monitor and secure critical infrastructure systems against potential disruptions.	**Expert**
321697	Ensure security by design in all system development processes to protect against cyber and physical threats.	**Expert**
322796	Operate SCADA systems securely and resiliently in the cloud to enhance critical infrastructure operations and data accessibility.	**Expert**
323133	Conduct QA tests to establish drift baselines and set acceptance thresholds for product quality assessment.	**Expert**
322341	Develop secure MCP client-server architectures to enhance data integrity and confidentiality in critical national infrastructures.	**Expert**
322277	Implement secure data-sharing protocols within dashboards to ensure compliance with national cybersecurity regulations for critical national infrastructure.	**Expert**
322161	Utilize edge computing to process data locally, reducing latency and enhancing security in IoT deployments.	**Expert**
322178	Implement secure data-sharing protocols to facilitate confidential information exchange between energy sector organisations.	**Expert**

Table 25: IT Engineers FOP

FOP Title IT Quality and Testing Professionals
Role Level Professional and Delivery
Required for supply chain partners Original Equipment Manufacturers (OEM's), Primes, Tier-1s; Small to Medium Enterprises (SMEs); RTO/COI - Research & Innovation Organisations; Equipment Service Providers; Regulatory Organisations

ID	Capability Statement	Proficiency
322824	Use AI generated interactive content to facilitate learning and training in safety standards	**Awareness**
323106	Demonstrate the application of zero-knowledge protocols within ERP and logistics planning solutions	**Awareness**
322794	Develop advanced cryptographic authentication mechanisms to securely bind digital twins to their corresponding physical assets.	**Awareness**
323127	Integrate automation suites to optimise, rationalise, and adopt component procurement strategies	**Awareness**
322807	Utilise AI-based forensic analysis to investigate and respond to cyber incidents affecting critical infrastructure.	**Awareness**
323133	Conduct QA tests to establish drift baselines and set acceptance thresholds for product quality assessment.	**Expert**
323139	Commission checklists and perform acceptance tests to ensure efficient deployment of hardware and software elements.	**Expert**
322048	Design and maintain SCADA testbeds to evaluate system security and performance under simulated conditions.	**Expert**
323123	Adopt AI solutions in the assessment of quality controls compliance for products	**Expert**
322826	Design processes for system prototypes to test AI failure scenarios to optimise and improve system reliability	**Expert**
323108	Demonstrate AI solution effectiveness in assessing product quality control compliance.	**Expert**
322815	Test IoT-enabled sensors to validate data collection accuracy and support predictive maintenance strategies.	**Expert**
322095	Establish secure testbeds for SCADA migration to validate system performance and security before deployment.	**Expert**
323131	Deploy safety hardware and software to ensure readiness for site commissioning and integration verification, meeting all acceptance criteria.	**Expert**
322817	Design test campaigns to include specific processes, input datasets, metrics, and clear criteria for success or failure.	**Expert**

Table 26: IT Quality and Testing Professionals FOP

FOP Title Mechatronic Engineers
Role Level Professional and Delivery
Required for supply chain partners Original Equipment Manufacturers (OEM's), Primes, Tier-1s; Small to Medium Enterprises (SMEs); RTO/COI - Research & Innovation Organisations; Equipment Service Providers

ID	Capability Statement	Proficiency
322824	Use AI generated interactive content to facilitate learning and training in safety standards	**Awareness**
322822	Use AI generated interactive content to facilitate specialised training in complex environments	**Awareness**
323116	Design interfaces to define clear roles and decision points between human staff, robots, and AI systems to enhance procedural efficiency and accountability.	**Awareness**
323138	Develop robotic technologies integrated with artificial intelligence in critical national infrastructure systems to provide specific physical monitoring or execute precise physical actions.	**Expert**
322823	Utilise advanced drones/robots to perform specific maintenance tasks in hazardous environments.	**Expert**
322795	Develop prototype IoT-enabled sensors to enhance data collection accuracy and support predictive maintenance strategies.	**Expert**
322815	Test IoT-enabled sensors to validate data collection accuracy and support predictive maintenance strategies.	**Expert**

Table 27: Mechatronic Engineers FOP

FOP Title Power Systems Engineers
Role Level Professional and Delivery
Required for supply chain partners Original Equipment Manufacturers (OEM's), Primes, Tier-1s; Small to Medium Enterprises (SMEs); RTO/COI - Research & Innovation Organisations; Equipment Service Providers

ID	Capability Statement	Proficiency
323112	Develop interoperability frameworks for critical national infrastructure to ensure secure data exchange between different systems.	**Awareness**
322799	Analyse facility energy demands and generation constraints to maximise the efficient utilisation of low carbon energy sources in specific operational sectors.	**Expert**
322800	Integrate assets and grid interfaces to improve efficiency, stability and renewable energy utilisation	**Expert**
189856	Using advanced computational modelling techniques to optimize energy generation processes.	**Expert**
322803	Integrate secure, resilient, and safety-governed remote control of electrical networks to support efficient operation.	**Expert**
322149	Integrate edge computing solutions to enhance real-time data processing and operational efficiency in energy systems.	**Expert**
322792	Integrate digital twin technologies with energy infrastructures to enhance resilience against cyber threats.	**Expert**

Table 28: Power Systems Engineers FOP

FOP Title Security Controls and Instrumentation Engineer
Role Level Professional and Delivery
Required for supply chain partners Original Equipment Manufacturers (OEM's), Primes, Tier-1s; Small to Medium Enterprises (SMEs); RTO/COI - Research & Innovation Organisations; Equipment Service Providers

ID	Capability Statement	Proficiency
322043	Integrate artificial intelligence-driven threat detection systems to proactively identify and mitigate cyber threats in critical national infrastructures.	**Awareness**
322343	Integrate MCP with existing security frameworks to strengthen resilience against cyber threats in energy sector infrastructures.	**Awareness**
322152	Design secure network architectures for critical infrastructure to prevent unauthorized access and ensure system resilience.	**Awareness**
322239	Implement AI-driven anomaly detection to identify and mitigate cyber threats in critical national infrastructure.	**Awareness**
322265	Integrate AI-driven surveillance systems to enhance real-time threat detection and response in critical national infrastructure facilities.	**Awareness**
322337	Implement zero-knowledge proof protocols to verify system integrity without exposing sensitive data.	**Awareness**
322802	Integrate tamper-resistant transaction and audit mechanisms to support secure energy markets and fraud detection.	**Awareness**
322199	Implement network segmentation to isolate SCADA systems from corporate IT networks and enhance security.	**Awareness**
322807	Utilise AI-based forensic analysis to investigate and respond to cyber incidents affecting critical infrastructure.	**Awareness**
323106	Demonstrate the application of zero-knowledge protocols within ERP and logistics planning solutions	**Awareness**
322791	Develop hardware solutions with industry partners to enhance security for critical national infrastructure, specifically by implementing Trusted Execution Environment technologies.	**Awareness**
322340	Utilise zero-knowledge proofs to enable secure, anonymous reporting systems in critical infrastructure networks.	**Awareness**
322794	Develop advanced cryptographic authentication mechanisms to securely bind digital twins to their corresponding physical assets.	**Awareness**
322179	Develop and deploy smart contracts to automate and enforce agreements within critical national infrastructures.	**Awareness**
322051	Encrypt data in transit and at rest to protect sensitive information within IoT networks.	**Awareness**
322797	Design security controllers for critical national infrastructure SCADA systems to improve specific operational metrics and guarantee consistent system performance.	**Expert**
322248	Maintain research-grade SCADA systems to support continuous innovation and development in critical infrastructure.	**Expert**
322048	Design and maintain SCADA testbeds to evaluate system security and performance under simulated conditions.	**Expert**
322814	Design security interfaces and decision-support tools to enable rapid, safe, and informed actions by critical national infrastructure activities.	**Expert**

323130	Implement chain of custody procedures to ensure secure handling of hardware and deploy calibration procedures to maintain accuracy in measurements.	**Expert**
322803	Integrate secure, resilient, and safety-governed remote control of electrical networks to support efficient operation.	**Expert**
322815	Test IoT-enabled sensors to validate data collection accuracy and support predictive maintenance strategies.	**Expert**
322065	Deploy AI-based predictive maintenance systems to proactively identify and address vulnerabilities in critical infrastructure components.	**Expert**
322793	Develop hybrid SCADA prototypes to validate interoperability between cloud-based services and existing operational technology systems.	**Expert**
322291	Integrate digital twins with IoT systems to enhance real-time monitoring and predictive maintenance of energy assets.	**Expert**

Table 29: Security Controls and Instrumentation Engineer FOP

Appendix D Background to the Workforce Foresighting Hub

Addressing future workforce challenges

The global marketplace is changing at a rapid pace, and the continued development of innovative technologies is creating opportunities for growth in all sectors.

Whilst we are well placed to take advantage in the UK, the Government and industry have identified that we need a workforce able to adapt to new capabilities that require different and often higher skill sets. The 'Manufacturing the Future Workforce' report, published in 2020, states: "Failure to address the workforce development challenge will mean missing out on opportunities to build the UK's manufacturing base and to take market leading positions."

Developing this workforce and preventing a skills shortfall will provide future-thinking organisations with the capabilities to successfully adopt innovation and enable the UK to build a prosperous economy.

The Skills Value Chain

A Skills Value Chain (SVC) approach promotes connectivity between upstream UK innovation and downstream skills systems, as well as enabling better co-operation within education and training provider eco-systems. It aligns and integrates innovation and skills strategies with a common purpose.

The SVC approach was proposed in the 'Manufacturing the Future Workforce' report, which examined global best practice and convened UK pioneers to explore how the UK can develop skills to exploit innovative technologies.

It starts with workforce foresighting.

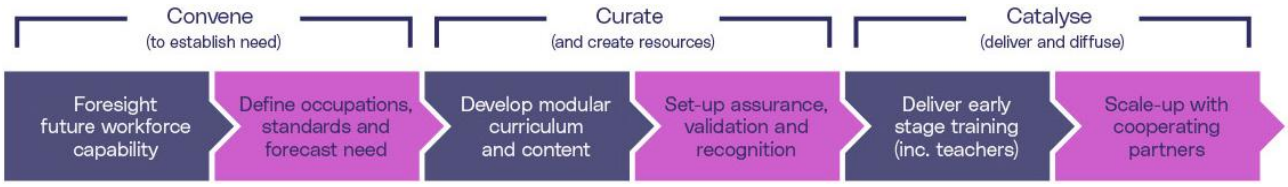

Figure 1: The Skills Value Chain (SVC)

Workforce foresighting

Using the Skills Value Chain approach, the UK will start building the skilled workforce required by tomorrow's industries and employers, and understanding what these future needs will be is where workforce Foresighting comes in.

Workforce Foresighting is a systemic approach to identifying the organisational capabilities and workforce skills necessary to enable industry to adopt and exploit innovative technologies which respond to global, national and sector challenges.

The Workforce Foresighting Hub, initiated and funded by Innovate UK, built in collaboration with the Catapult Network, provides the processes and data that inform insight and supports the recommendations required for industry, policymakers, and educators to respond to continuing change.

Our Vision: To foster the organisational capabilities and workforce skills required to adapt to continuing change and enable adoption of innovative technologies to enable a prosperous UK industry.

Our Mission: To provide the process, insight and recommendations required to identify and address future skills demands to enable the UK to adopt innovation and succeed in the dynamic global marketplace.

Our Goals:

Define future capabilities required across a sector in response to a challenge, or technology innovation and consequently define the skill sets of the workforce of the future.
Understand and explain gaps between technology adoption, organisational capability, and workforce profiles that could hamper innovation.
Identify and communicate insights, future requirements and the action required by industry and educators.
Enable and deliver a consistent approach to workforce Foresighting.

Outcomes:
The process integrates insight from experts in three categories – domain specialists/technologists, employers, and educators. Using a structured and facilitated series of collaborative information-gathering workshops, combined with data from open-source global data sets, the workforce Foresighting process can produce a wealth of detailed quantitative data to inform action.

At the heart of the Foresighting process are working groups consisting of the industry sponsor and centre of innovation, with support from the Workforce Foresighting Hub team, who undertake detailed analysis to report and summarise key data insights and

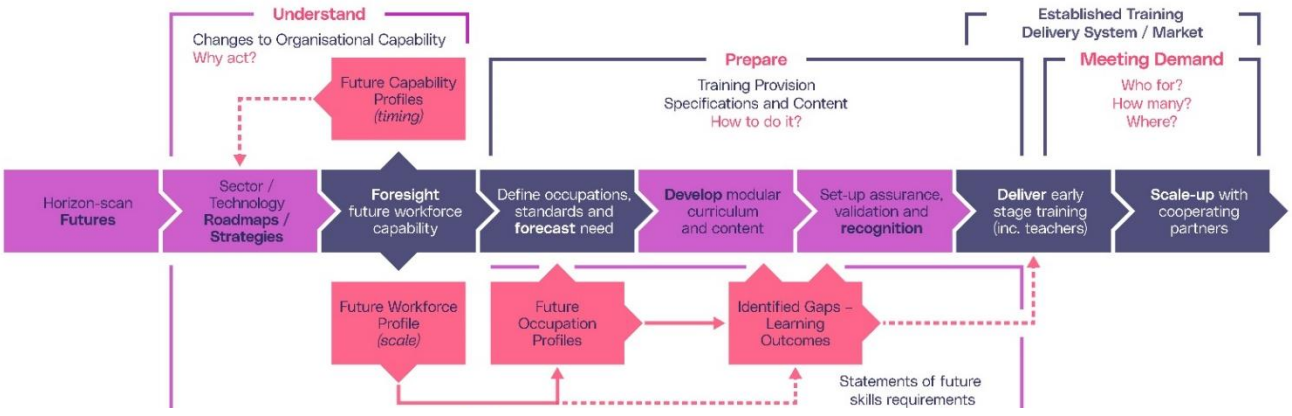

Figure 4: Workforce Foresighting & Skills Value Chain

recommendations for action. This report details future supply chain capabilities, prototype FOPs and identifies changes required to current training provision for the sponsor to take forward and address skills challenges relating to the specific topic.

Approach used - principles and implementation

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. Lists of workshop participants are provided in Section 1.3 (**1.3 Contributing Participants**)

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, classification enables data from a number of other national and international open-source workforce datasets to be integrated through the same common language. This 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 WFH team are constantly evolving and improving the detailed workshop process and workshop approach, but essentially 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 an actionable 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

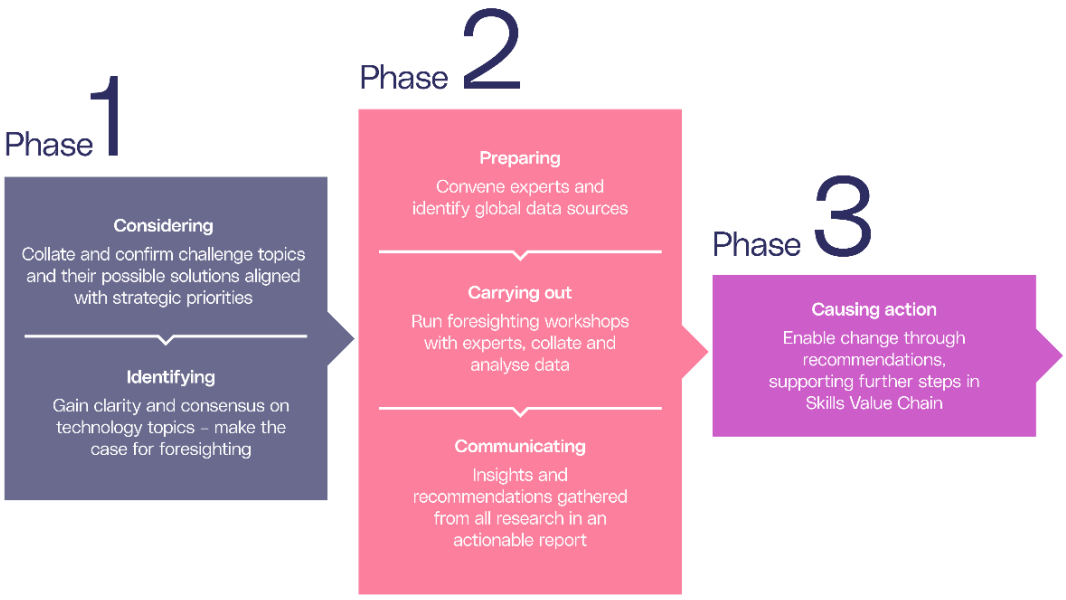

Figure 5: The workforce foresighting process

Forecasting and Foresighting

The result of workforce foresighting is understanding why skills requirements will need to change to enable the adoption of innovative technologies, and to define what this change is likely to be in terms of future occupations and shorter-term skills gaps. Forecasting of demand can then take these future focused findings and work with industry and government stakeholders to estimate the quantity of workers necessary for an industry to fulfill emerging skill demands at a given time and place. The two approaches are linked in that workforce foresighting identifies the requirements and forecasting can then determine the quantity needed; the people need the skills and therefore prepare programmes to deliver them.

Outcomes - insights and recommendations

Workforce foresighting cycle is a data intensive approach that can provide sponsors, stakeholders, and participants with detailed insight about future workforce requirements. A dynamic data set is provided for each cycle to allow all stakeholders and participants to freely access and interrogate the data. Additionally, the WFH team will support the production of a report that provides targeted recommendations that require action to address gaps in training and education provision relevant to the challenge and planned technology solution.

The dynamic data portal provides a range of standard data sets and visualisations. Additionally, users can download data to undertake their own more detailed interrogation of data to guide and inform subsequent actions.

The key aspect is to provide insight about gaps – which capabilities required in the future are NOT addressed by aspects of current provision – apprenticeship standards, qualifications, or other provision. Gaps represent:

- **Short term CPD** – topics required across the workforce to upskill members of current workforce
- **Medium term** – topics to be included as current provision / standards are reviewed and updated
- **Longer term** – new qualifications and standards that may be needed to equip new entrants

The insight produced by a workforce foresighting cycle (project) provides:

- **Technologists** and technical leads with insight of the organisational capability sets required across future supply chain partners in response to the identified challenge.
- **Employers** with insight about possible future roles and occupations that may be required across the whole workforce, operators to researchers, to ensure they are equipped and ready.
- **Educators** with details of the gaps to be addressed by short-course training to upskill the existing workforce and also insight about qualifications and provision that will be required to support new entrants in the future.