Transforming Forensics

Programme Management Office

BUSINESS CASE – TF DIGITAL

Doc No: G960-TFP-KBR-PRG-AD-BUC-0042

TRANSFORMING FORENSICS Programme

The Transforming Forensics Programme SharePoint site holds the current version of this document.

Document Control

0.4	31/1/18	Updated following review	KBR	HA/LA		
0.3	29/01/18	Complete Draft	TF	MB-P		
0.2	15/01/18	Updated to reflect comments	TF	MB-P		
0.1	05/01/18	Strategic Case only	TF	MB-P		
Rev	**Issue Date**	**Reason for Issue**	**Organisation**	**By**	**Check**	**Approve**

Distribution List

Rev	**Date**	**Name**	**Organisation**

Abbreviations and Acronyms

Abbreviation	Meaning
APCC	Association of Police and Crime Commissioners
BDA	Business Design Authority
BI	Business Intelligence
CAID	Child Abuse Image Database
CCTV	Closed Circuit Television
CJS	Criminal Justice System
CMM	Capability Maturity Model
CPIA	Criminal Procedure and Investigations Act
CPS	Crown Prosecution Service
CSE / CSI	Crime Scene Examiner / Crime Scene Investigator
CSF	Critical Success Factors
DF	Digital Forensics
DII	Digital Investigation and Intelligence
DNA	Deoxyribonucleic acid
DOS	Digital Outcomes and Services (Framework)
EPB	Executive Programme Board
ESMCP	Emergency Services Mobile Communications Programme
FBC	Full Business Case
FCN	Forensic Capability Network
FRS	Financial Reporting Standard
FSP	Forensic Service Provider
FSR	Forensic Science Regulator
GDPR	General Data Protection Regulation
HM	Her Majesty's
HMCTS	Her Majesty's Courts and Tribunals Service
HMRC	Her Majesty's Revenue and Customs
HOB	Home Office Biometrics
HTCU	Hi-tech Crime Unit
ICT	Information and Communications Technology
ISO	International Standards Organisation
KBR	Kellogg Brown and Root
MI	Management Information
MSP	Managing Successful Programmes
S23(1)	*S23(1)*
NLEDS	National Law Enforcement Data Services
NPCC	National Police Chiefs' Council
OBC	Outline Business Case

OEM	Original Equipment Manufacturer
OGC	Office for Government Commerce
PCC	Police and Crime Commissioner
PER	Project Evaluation Review
PIR	Post-Implementation Review
PMO	Programme Management Office
PoC	Proof of Concept
PRINCE	Projects in a Controlled Environment
PTF	Police Transformation Fund
PRTB	Police Reform and Transformation Board
R&D	Research and Development
RAID	Risks, Assumptions, Issues and Dependencies
SOC	Strategic Outline Case
SOP	Standard Operating Procedure
SRO	Senior Responsible Owner
TDA	Technical Design Authority
TF	Transforming Forensics
TFP	Transforming Forensics Programme
TRL	Technology Readiness Level
TUPE	Transfer of Undertakings (Protection of Employment)
UK	United Kingdom of Great Britain and Northern Ireland
UKAS	UK Accreditation Service
VAT	Value Added Tax
VfM	Value for Money
VMOST	Vision, Mission, Objectives, Strategies and Tactics
YatH	Yorkshire and the Humber (Policing Region)

1. Executive Summary

1.1 The Strategic Case

1.1.1 Introduction

This business case **(Strategic Outline Case) is for the investment of £4,000,000** during the period from April 2018 to March 2020 to **establish a national approach and roadmap for the development and management of an integrated, future-proofed digital forensic science capability** for policing in England and Wales.

For the purposes of this business case, digital forensic science (digital forensics) is defined as "the acquisition, preservation, analysis and presentation of digital data for evidential use in the criminal justice system".

The business case is one of a series forming part of the broader Transforming Forensics (TF) Programme.

1.1.2 The Strategic Context

The proliferation of digital devices, the expansion of digital storage and the pace of change of digital technologies have made **digital forensics the fastest growing and fastest changing area of forensic science**.

Every single crime investigation in the United Kingdom is now likely to have some form of digital element, be this **analysis of a phone** for checking a person's stated whereabouts or record of events; analysis of **digital evidence recorded by a witness or on CCTV footage**; analysis of **computers, Wi-Fi routers, satellite navigation or vehicle telemetry systems**; or indeed analysis of **databases, computer networks and cloud storage**. **A growing number of crimes**, of course, **are perpetrated completely digitally** and their criminal investigations will rely almost **exclusively upon digital forensic capabilities**. At the same time, **digital forensics produces a particularly strong form of evidence** and one that has a significant impact upon both criminal justice outcomes and their efficiency. Over 90% of people arrested for child sexual exploitation offences, for example, **plead guilty** once the initial digital forensics evidence has been presented to them.

In 2015-16 police forces in England, Wales and Northern Ireland, including the British Transport Police and the*S23(1)*, **spent an estimated £74 million on digital forensics and examined approximately 200,000 digital devices**; these figures are estimated by the Home Office to be **rising by approximately 29% each year**. The Transforming Forensics Outline Business Case, prepared in March 2017, estimated that, **without a fundamental change in the operating model, the cost of digital forensics to police forces in England, Wales and Northern Ireland could reach £162 million per annum by 2022-23**.

That is, of course, if police forces are both able to afford such increases and identify sufficient capacity, either internally or externally, to deal with the demand. **Processing backlogs in some areas are already significant, with turnaround times often stretching to many months**. Some digital forensic examinations are not progressed as a result, which can easily lead to a gradual **erosion of public confidence in policing**.

The Transforming Forensics Programme, to which this Digital Forensics project belongs, has been carefully designed to support the delivery of the UK Policing Vision 2025 and the Home Office's Forensic Science Strategy (March 2016). The Transforming Forensics Vision is:

"To deliver high quality, specialist forensic capabilities, in support of the Policing Vision 2025, to rapidly protect communities and the vulnerable, which are sustainable to meet future threats and demand."

The TF Digital Forensics project is designed to work closely with TF and other national programme stakeholders to:

- achieve a shared vision and a collaborative approach;
- create a sustainable national capability;
- develop and inspire people;
- ensure long-term sustainability.

Full details of how the project is intending to achieve this and how it aligns with both Policing Vision 2025 and the Home Office's Forensic Science Strategy are set out in chapter 2.

1.1.3 The Case for Change

The need for a specific Digital Forensics project, as part of the broader Transforming Forensics Programme, is based upon 6 main drivers for change. These are explained in detail in section 2.6. In summary, they are:

1. The **current arrangements** for digital forensics across policing **are fragmented, sub-optimal, carry inherent risk and are out of alignment with both Policing Vision 2025 and the Home Office's Forensic Science Strategy**.
2. The **pace of change** in digital forensics and the **growing demand** for its capabilities **are too great for police forces to tackle individually**.
3. The **nature of digital technology, the ways in which it is supported and the standards against which it is measured are changing, necessitating a different approach from policing and providing new opportunities**.
4. The **importance of digital technology**, and indeed the **digitisation of many traditional forensic processes** and information, **requires much more integration of digital and traditional forensics capabilities** than was previously required.
5. Police forces have **significant data protection and disclosure obligations**, which are currently proving challenging to meet, either reliably or cost effectively, and **will become more demanding when the General Data Protection Regulation (GDPR)** comes into force on 25th May 2018. This is especially difficult in relation to **the 'right to be forgotten'.**
6. Without a bespoke Digital Forensics project, **the potential benefits and opportunities associated with the national Digital Intelligence and Investigation (DII) Programme, and indeed the Home Office Biometrics (HOB) Programme, are unlikely to be maximised**.

1.2 The Economic Case

1.2.1 The Options Considered

A long-list of 11 options was considered, as set out in section 3.4. These were reduced to a short-list of 6.

Option	Description
1	Do nothing and leave forces to develop their own capabilities using existing governance and collaborative structures
2	Establish an in-house / police-led advisory capability with the limited scope of supporting forces with the implementation of the findings of the "Enabling Digital Forensics" Proof of Concept project (extraction of digital data from devices using kiosks) and with their ISO 17025 and ISO 17020 accreditation challenges
3	Establish an in-house / police-led advisory capability with a much broader scope, building upon Option 2 but including all techniques & capabilities involving the acquisition, preservation, analysis & presentation of digital data for evidential use in the CJS
4	Establish an in-house delivery service, designed to provide digital forensic science services to police forces across England, Wales and potentially Northern Ireland
5	Establish an in-house / police-led advisory capability with the scope of Option 2 but with the additional remit to determine whether there is a business case to deliver the corresponding services to police forces across England, Wales and potentially Northern Ireland
6	Establish an in-house / police-led advisory capability with the scope of Option 3 but with the additional remit to determine whether there is a business case to deliver the corresponding services to police forces across England, Wales and potentially Northern Ireland

1.2.2 The Preferred Option

At Strategic Outline Case stage, a business case is only designed to crystallise a "preferred way forward". At the next stage of business case development (Outline Business Case), options could be refined or modified, based upon new information. As part of its evaluation therefore, the project team has been careful to recommend a "preferred way forward", which will provide maximum benefit without restricting future potential opportunities. Using this approach, the preferred way forward is Option 6, whose scope is to:

- Establish an in-house / police-led advisory capability covering all techniques and capabilities involving the acquisition, preservation, analysis and presentation of digital data for evidential use in the criminal justice system, which will work closely with the Digital Policing Portfolio (including the DII and Digital First programmes), to ensure cohesion of service operating models and
- Undertake the research and engagement needed to produce a comprehensive Outline Business Case to determine whether it would be beneficial to rationalise, aggregate or integrate into a national Forensic Capability Network any of the digital forensic capabilities that are currently delivered by individual police forces or groupings.

The reasons for choosing this option are set out in detail in section 3.5. In summary, Option 1 was rejected because it would do nothing to address the challenges currently faced by policing. Options 2 and 5 were rejected because their scope was deemed to be too limited, especially given the synergies with the Digital Intelligence and Investigation and Digital First programmes. Option 4 was rejected for the time being because it could only currently focus upon the extraction of data from digital devices and there are already contracts in place enabling forces to progress these capabilities. Options 3 and 6 were therefore best placed, with Option 6 being preferred since it recognises the potential for joined-up delivery of some

digital forensics capabilities as part of a broader Forensic Capability Network[1], as well as the need to undertake much greater analysis of the digital forensics landscape before being able to make any definitive recommendations about changes to the delivery landscape.

1.2.3 Expected Benefits

The Digital Forensics project is expecting to deliver very significant financial and non-financial benefits. The level of expected financial benefits will be crystallised at Outline Business Case stage. However, the project estimates that annual savings of at least 20% could be achieved in digital forensics by adopting a "Forensic Capability Network" approach, investing in greater automation capabilities and improving the overall operating model. With spending on digital forensic science soon expected to exceed £100 million per annum, the Digital Forensics project will be targeting ongoing financial savings of at least £20 million per annum. The expected non-financial benefits of the project include:

Expected Benefit	Estimated Delivery
Cohesive strategic direction and a bespoke science and technology roadmap, ensuring services are up-to-date and aligned with other national programmes	From 2018 onwards
Nationally defined and agreed digital forensic specifications and standards, which will greatly benefit accreditation, procurement and integration with other departmental roadmaps, as well as the interface between forensics, investigations and the criminal justice system	From 2019 onwards
Reduced risk through cohesive governance and management of forensic provision	Blueprint scheduled for delivery during 2019, with new landscape by 2025 at the latest
Long-term sustainability of digital forensic services, with capabilities closely aligned with demand and access to expertise	Blueprint scheduled for delivery during 2019, with new landscape by 2025 at the latest
Better value for money by having an ecosystem of expertise, meaning that forces do not all have to maintain a cadre of the same specialist posts	Blueprint scheduled for delivery during 2019, with new landscape by 2025 at the latest
Better value for money by achieving economies of scale and a less fragmented digital forensic service and supply chain, as policing speaks with one voice in commercial negotiations and with regards to Research and Development priorities	From 2019 onwards
Increased productivity for policing, enabled by consistent and transparent performance management and the use of clear and transparent service levels against nationally agreed outputs, linked to policing outcomes	From 2019 onwards
Integration of digital and traditional forensic capabilities, with the ability to cross-fertilise skills	From 2019 onwards

[1] Forensic Capability Network – the creation of a national network of forensic capabilities, achieved by linking, combining and harmonising existing police force capabilities into a configuration that enables demand to be shared and load-balanced across the country, as needed.

Expected Benefit	Estimated Delivery
across the workforce	
Future proofed science and technology offering best of breed services, backed up by a robust R&D capability and an agreed development roadmap	From 2019 onwards
More effective engagement with Original Equipment Manufacturers (OEMs), providing appropriate access to data and technical support	From 2018 onwards

1.3 The Commercial Case

1.3.1 Procurement Strategy

The project's procurement strategy is to use a combination of in-house policing expertise, which will be sourced through secondments, and external expertise, which will be delivered through the existing TF Programme Delivery Partner contract, procured using the Digital Outcomes and Services (DOS2) Framework by Dorset Police. Further procurement activity will be undertaken under the guidance of Dorset Police and the National Police Procurement Lead for Forensics.

1.3.2 Required Services

At this stage of the Digital Forensics Project, the proposal involves the creation of a "Digital Forensics Advisory Team", which will work with the National Police Chiefs' Council (NPCC) Digital Forensics Board and the DII Programme to:

- establish a national authority for Digital Forensics with leadership over technical requirements, quality and processes;
- construct a detailed baseline of force digital forensic capabilities and initiatives, including contracts, procurement and change projects, and make equivalent assessments of demand;
- forge effective public / private / academia partnership to undertake research into future capabilities (emerging and potential) to inform future focus and investment;
- cover the appropriate breadth and depth of digital forensics expertise to support forces in meeting their 'digital forensic' challenges;
- create, along with the DII Programme, a service operating model for a broad range of investigative / forensics scenarios, providing clarity on capabilities and techniques and how best to deploy them;
- work with forces to address current shortfalls in digital forensic support skills, notably the availability of technicians to support frontline digital forensic services;
- create effective links with OEMs to gain access to appropriate data and technical support;
- work with forces and other stakeholders to create a catalogue of approved / endorsed capabilities and techniques;
- work with forces, the Forensic Science Marketplace Group and the Police ICT Company to help procure new capabilities / rationalise existing capabilities;
- support forces with short-term ISO17025 and medium-term ISO17020 accreditation activities (aligned to the related Standards and Accreditation Project);
- define and construct the Digital Forensics elements of the TF learning and development programme;
- represent forces and work with the FSR to produce quality standards, operating models and codes of conduct, which can keep pace with digital forensics;
- produce recommendations, supported by a business case, for the creation of a resilient and future-proofed network of digital forensic capabilities, forming part of an integrated forensics capability and incorporating networking arrangements for evidence management and sharing of intelligence, aligned to the agreed service operating model;

- design a new funding model to support a sustainable, consistent, integrated, quality assured network of digital forensic capabilities.

1.3.3 Potential for Risk Transfer and Potential Payment Mechanisms

There is scope within the existing Delivery Partner contract for specific deliverables to be commissioned on a fixed price basis, and this option will be exercised where it is likely to offer best value. A similar approach will be adopted for other procurements, with the proposed payment mechanism being aligned to the risk transfer arrangements deemed to offer the optimum solution to policing.

1.4 The Financial Case

1.4.1 Financial Expenditure

The estimated cost of supporting Option 6 during the period from April 2018 to March 2020 i.e. the period covered by the Police Transformation Fund is set out below.

Cost Heading	2018/19 £'000	2019/20 £'000	Total £'000
Digital Forensics Advisory Team	594	1,456	2,050
Business & Technical Leadership, Analysis, Design & MI / BI	235	616	851
Business Case, Funding Model & Procurement / Sourcing	167	240	407
Project Management, Business Change, Training & Communications	254	438	692
Totals	**1,250**	**2,750**	**4,000**

1.4.2 Overall Affordability and Balance Sheet Treatment

The proposal is to fund the Digital Forensics project, as currently defined, exclusively from grant and it will therefore have no impact upon participating forces' income and expenditure accounts or balance sheets. The Outline Business Case, which is scheduled to be produced by the end of 2018, will provide a comprehensive schedule of recommended investment and expected benefits beyond March 2020. Overall affordability of the longer-term business case is expected to be extremely positive, given the significant affordability challenges currently faced by police forces with the existing operating model.

1.5 The Management Case

1.5.1 Project Plan and Project Management Arrangements

The illustrative plan to deliver the services set out in 1.3.2 is depicted below.

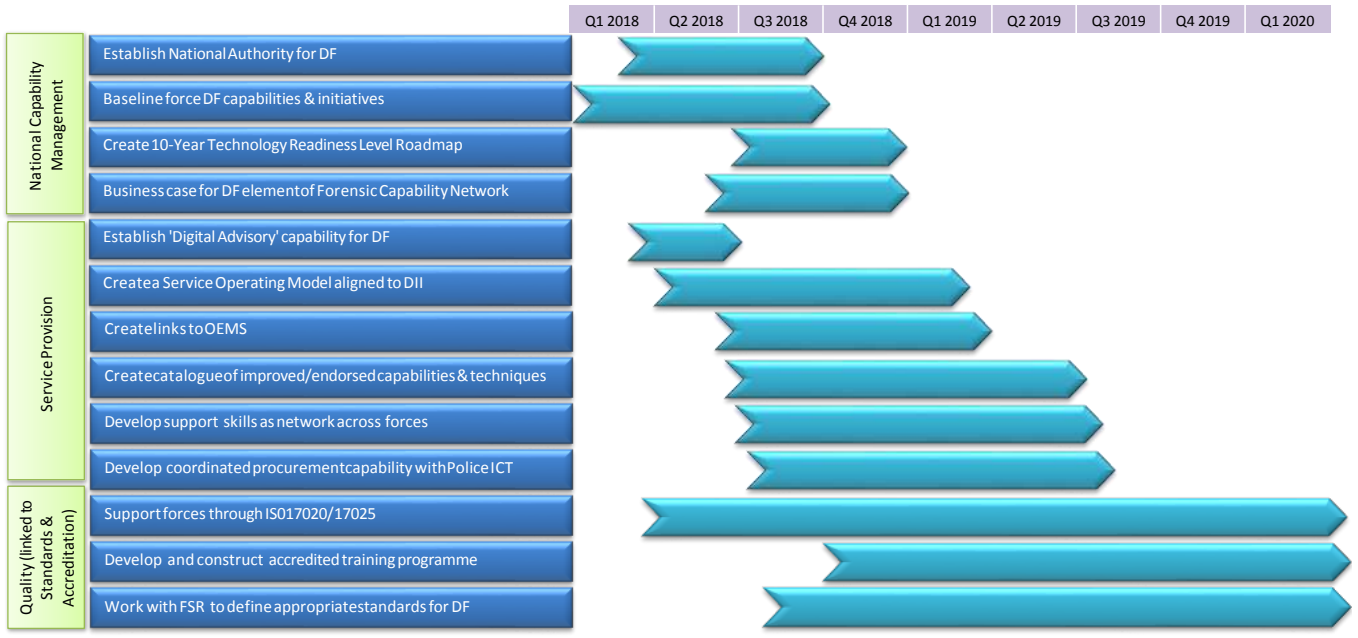


Figure 6 – Illustrative Project Plan

The project will be managed using PRINCE2 best practice methodology, as well as MSP (Managing Successful Programmes) as part of the overarching Transforming Forensics Programme. Further details of these arrangements, together with their governance and reporting structures and how they fit within the broader Police Reform and Transformation landscape, are set out in sections 6.2 and 6.3.

1.5.2 Benefits Realisation and Risk Management

The overall approach for the TF Programme and its constituent projects is benefits-focused. A Benefits Management Strategy has been prepared and a robust benefits realisation plan is being developed and will be monitored throughout the programme's lifecycle. Further details are set out in section 6.6. The TF Programme is also being supported by dedicated "business readiness and change managers", who will be responsible for monitoring the early benefits as they are delivered by both the programme and participating forces. As the programme develops, the benefits will be handed over to operational owners with responsibility for realising the benefits in their areas.

The TF Programme has adopted a very rigorous and professional approach to RAID (Risk, Assumption, Issue and Dependency) management, with the Programme Review Board keeping them under constant review. The most significant risks facing the Digital Forensics Project are set out within the Strategic Case (section 2.9) and the programme's risk management arrangements are set out in further detail in section 6.5.

1.5.3 Post Project Evaluation Arrangements

The TF Programme has put in place arrangements for both a Post-Implementation Review (PIR) and a Project Evaluation Review (PER). The PIR will appraise how well the project was managed and whether it delivered to expectations. The PER will ascertain whether the anticipated benefits have been delivered. Both will be undertaken by an Independent Evaluation Team, which will be appointed with support from the Home Office Crime Analysis Unit and Government Trials Advisory Panel.

1.6 Recommendation

It is recommended that, subject to the Transforming Forensics Programme securing the requested £30.35 million grant from the Police Transformation Fund, £4 million is invested in a Digital Forensics Project to create a team that can work with the NPCC Digital Forensics Board and DII Programme over the next 2 years to **establish a national approach and roadmap for the development and management of an integrated, future-proofed digital forensic science capability** for policing in England and Wales.

2. The Strategic Case

2.1 Introduction

This business case (Strategic Outline Case) is for the investment of £4,000,000 during the period from April 2018 to March 2020 to establish a national approach and roadmap for the development and management of an integrated, future-proofed digital forensic science capability for policing in England and Wales.

For the purposes of this business case, digital forensic science is defined as "the acquisition, preservation, analysis and presentation of digital data for evidential use in the criminal justice system".

The business case is one of a series of business cases forming part of the broader Transforming Forensics (TF) Programme. Appendix A provides a schedule of all the current business cases in the series.

2.1.1 Structure and Content of the Document

This business case has been prepared using the agreed standards and format for business cases, as set out in HM Treasury "The Green Book (Appraisal and Evaluation in Central Government)".

The approved format is the Five Case Model, which comprises the following key components:

- the strategic case, which sets out the strategic context and the case for change, together with the supporting investment objectives for the scheme.
- the economic case, which demonstrates that the organisation has selected the choice for investment, which best meets the existing and future needs of the service and optimises value for money (VFM).
- the commercial case, which outlines the content and structure of the proposed deal / commercial arrangements.
- the financial case, which confirms funding arrangements and affordability and explains any impact on the balance sheets of the participating organisations.
- the management case section, which demonstrates that the scheme is achievable and can be delivered successfully to cost, time and quality.

At this stage of business case (Strategic Outline Case), the 5 cases above are only partially completed and the aim of the business case is to reach a "preferred way forward". A preferred option or design for any future reshaping of the digital forensics landscape will only be reached at Outline Business Case stage, which for this project is scheduled for the end of 2018.

The purpose of this section (the strategic case) is to explain how the scope of the proposed project fits within the existing business strategies of the participating organisations and to demonstrate a compelling case for change, in terms of existing and future operational needs.

2.2 Organisational Overview

This business case forms part of the Transforming Forensics Programme (TFP), which is being delivered on behalf of the Association of Police and Crime Commissioners (APCC) and the National Police Chiefs' Council (NPCC) as part of its Reform and Transformation portfolio. TFP is one of the 4 largest police transformation programmes within that portfolio. It operates on an "opt-in" basis and currently has sign-up from 44 of the United Kingdom's policing / law enforcement organisations, as illustrated by the map below.

Figure 1 – Force / Law Enforcement Participation

2.3 Business Strategies

The Transforming Forensics Programme, to which the Digital Forensics project belongs, has been carefully designed to support the delivery of the UK Policing Vision 2025 and the Home Office's Forensic Science Strategy March 2016.

The UK Policing Vision 2025 describes a future where:

- the link between communities and the police will continue to form the bedrock of British policing. **Local policing** will be tailored to society's complex and diverse needs – with the delivery of public protection being informed by community priorities and robust evidence-based demand analysis;
- our **specialist capabilities** will be better prepared to respond to existing and emerging crime types. Decisions on how capabilities are positioned, structured and deployed will reflect the need to rapidly protect communities and the vulnerable, as well as provide value for money;
- the police service will attract and retain a **workforce** of confident professionals able to operate with a high degree of autonomy and accountability and will better reflect its communities;
- **digital policing** will make it easier for the public to contact the police wherever they are in the country, enabling us to make better use of digital intelligence and evidence and transfer all material in a digital format to the criminal justice system;
- policing will be agile and outward focused. Police forces and their partners will work together in a consistent manner to enable **joined up business delivery** around policing support services and community safety;
- clear **accountability arrangements** will support policing at local, cross-force and national levels. This will ensure that there is coherence between the oversight of the police reform programme and local policing and crime plans, as well as developing arrangements that recognise the roles of different policing bodies. Police and Crime Commissioners (PCCs) will continue to be at the heart

of engaging communities in the reform plans so that the public understand and have confidence in any change.

At the heart of creating this new future is **making transformative change** across the whole of policing with a keen focus upon the public and improving services for them. Central to this is a focus upon **inspiring the people who work in policing and working with them** to create the capabilities, systems and processes that will enable them to provide the first-class services members of the public deserve.

The Home Office's Forensic Science Strategy sets out a vision for forensic science, based upon a national approach to forensic science delivery in the criminal justice system and focusing upon ensuring quality standards and proper ethical oversight, improving value for money and strengthening public and judicial trust in forensic science.

Drawing together both Policing Vision 2025 and the Home Office's Forensic Science Strategy, t**he Transforming Forensics Vision**, as agreed with the programme's broad range of stakeholders, is:

"To deliver high quality, specialist forensic capabilities, in support of the Policing Vision 2025, to rapidly protect communities and the vulnerable, which are sustainable to meet future threats and demand."

The Transforming Forensics Programme Business Case provides a comprehensive analysis of how the TF Programme, as a whole, supports each of these elements of the future vision.

In the context of this particular project business case, the key elements of alignment are reflected below:

The Link between Communities and the Police will continue to be the bedrock of British policing.

The TF programme has been built upon the premise of policing by consent and recognises the need to embed legitimacy, trust and confidence, underpinned by the Code of Ethics, in all it does. The programme is therefore placing significant emphasis both upon making it easy for members of the public to help the police and delivering outcomes that instil confidence. The Digital Forensics project will play two key roles in this regard. Firstly, it will support the development of the capability in line with an accredited and standards led environment which will align to the public contact aspect of the DII programme to enable police forces to be able to accept digital evidence from members of the public without having to take possession of their digital devices. Secondly, it will help ensure that police forces have clarity, advice and support regarding the techniques and capabilities needed to acquire, preserve, analyse and present digital data for evidential use in the criminal justice system, in a way that meets all associated accreditation standards. To remain relevant in modern society, policing needs to police the digital domain as effectively as it does the physical one.

Specialist capabilities will be better prepared to respond to existing and emerging crime types. Decisions on how capabilities are positioned, structured and deployed will reflect the need to rapidly protect communities and the vulnerable, as well as provide value for money.

TF is providing or enhancing a series of specialist capabilities and services that can be accessed by any law enforcement organisation and centre around victims and public protection. The Digital Forensics project is tackling the largest and most significant crime growth area and will establish a national approach and roadmap for the development and management of an ecosystem of integrated, future-proofed digital forensics capabilities that are able to support policing throughout England and Wales. The capabilities to be developed, accredited and delivered will enable more effective investigations, prevent crime and protect communities. In doing so, the Digital Forensics project will also support the principles of improving safeguarding and reducing victimisation, and thereby enable an improved victim support service.

The police service will attract and retain a workforce of confident professionals.

Effective digital forensics acquisition, analysis and interpretation / attribution require a highly skilled workforce, able to meet local and national needs, often in very short timescales. Through the Digital Forensics project, allied to 3 other TF projects focusing upon fingerprint capabilities, next generation DNA analysis and standards and accreditation, TF will help law enforcement organisations (providing information and insight into the people, skills and knowledge aspect of the DII programme) attract and retain a workforce of confident professionals, able to meet the Forensic Science Regulator's accreditation standards and support and enable swift implementation of innovative forensic capabilities.

Policing will be agile and outward focused. Police forces and their partners will work together in a consistent manner to enable joined up business delivery.

TF is targeting positive impact across the whole criminal justice system, focused on delivery across the entire supply chain, from crime scene to court. The Digital Forensics project is designed to deliver significant enhancements to digital forensic capabilities and will work very closely with other law enforcement agencies e.g. Her Majesty's Revenues and Customs (HMRC), the Crown Prosecution Service (CPS) and HM Courts and Tribunals Service (HMCTS), together with commercial suppliers, Forensic Service Providers (FSPs) and the Forensic Science Regulator (FSR), to ensure that these new capabilities yield maximum impact in deterring and preventing crime, bringing offenders to justice and keeping people safe.

Clear accountability arrangements that recognise the roles of different policing bodies, coherence in the oversight of the police reform programme and PCCs continuing to be at the heart of engaging communities.

As set out in the Management Case of the TF Programme Business Case, the Transforming Forensics Programme has set up programme governance arrangements which involve key stakeholders across Law Enforcement, the Crown Prosecution Service (CPS), the Forensic Science Regulator (FSR), Her Majesty's Revenue and Customs (HMRC) and Her Majesty's Courts and Tribunals Service. TF is closely aligned with other significant transformation programmes, including the Home Office Biometrics (HOB) Programme, the Emergency Services Mobile Communications Programme (ESMCP), the National Law Enforcement Data Services (NLEDS) Programme and the Digital Policing Programmes.

The TF Digital Forensics project is working closely with the Digital Investigation and Intelligence (DII) Programme to ensure consistency, shared effort and maximum synergies. Both the TF and DII programmes report to the NPCC's Executive Review Board.

2.4 Investment Objectives

Supporting both the 2025 UK Policing Vision and the Home Office's Forensic Science Strategy is the Transforming Forensics Programme's own Vision (see 2.3 above), Missions, Objectives, Strategies and Tactics (VMOST).

The Programme Vision is organised around 4 mission statements, which also serve as overarching investment objectives:

- Investment Objective 1 – Achieving a shared vision and a collaborative approach;
- Investment Objective 2 - Creating a sustainable national capability;
- Investment Objective 3 - Developing and Inspiring people;
- Investment Objective 4 - Ensuring long-term sustainability.

This Digital Forensics project has been designed to support each of these investment objectives in the following way.

Achieving a Shared Vision and a Collaborative Approach:

- The project will involve the stakeholder community at every stage of the direction setting, design and implementation stages of the project by working with the Digital Intelligence and Investigation (DII) programme, participating police forces and the FSR to help create a service operating model to deliver in-scope digital forensic services, and a roadmap and a catalogue of approved capabilities and techniques that both meet policing's needs, as evidenced by a minimum 50% police force uptake of TF Digital Forensics offerings, and comply with the FSR's accreditation requirements.
- The project will respect local demand whilst building a coherent national solution – the catalogue of approved capabilities and techniques to be progressed through this project will be based upon national availability but to be provided or consumed by police forces and other law enforcement organisations in line with local capacity and demand.
- The project will contribute to and learn from the success of other police transformation programmes – progression of this project will be closely co-ordinated with that of the DII Programme.

Creating a Sustainable National Capability:

- The project will be supported by an appropriate governance framework – overarching governance of all forensic capabilities, both during and beyond project implementation, is an integral part of the TF Programme business case and the associated recommendations, as they relate to digital forensics, are reflected in this business case.
- The project will be supported and sustained by an appropriate funding model – the project's proposals, which reflect both the existing baseline for digital forensics and the overarching governance framework referenced above, are set out in the commercial and financial cases of this document and are designed around the principles of fairness and equity.
- The project will play its part in ensuring that all forensic capabilities are available to all policing organisations by nurturing and sustaining a viable ecosystem of digital forensic capabilities – digital forensic capabilities are complex, fast moving and will require targeted investment; they are also provided through a combination of in-house capability and external forensic service provision. Three of the key outputs from this project will be a sustainable funding model, a 10-Year Technology Readiness Level (TRL) roadmap (by 2019) and a funding pipeline (by 2022) for research and development, aimed at increasing R&D investment to a minimum of 3% of national spending by 2020 and a minimum of 5% by 2025.
- The project will be flexible to changing needs and requirements – digital technologies are constantly evolving, and the main objective of this project is to establish a national approach and roadmap for the development and management of an integrated, future-proofed digital forensics capability for policing in England and Wales.
- The project will accommodate individual forces' needs and priorities – this project, in common with all TF projects, is designed to ensure availability and consistency across a broad range of digital forensic capabilities but with individual forces able to invest in them according to their individual needs and priorities.
- The project will play its part in inspiring public confidence and trust by enhancing the credibility and legitimacy of all forensic products – standards and accreditation are core components of this project, both by helping forces with their immediate and individual accreditation responsibilities and by developing a catalogue of approved capabilities and techniques that have FSR endorsement.
- The project will provide demonstrable value for money and improved efficiency, including a minimum 25% reduction in direct costs per case outcome and a 50% reduction in the time and cost involved with forensic accreditation. Employing traditional "bit by bit imaging" techniques to acquire digital forensic evidence will become cost and time-prohibitive as the volumes of digital data continue to rise; this project will therefore explore and validate techniques that are more cost-effective whilst still meeting accreditation standards; it will also reduce the time and cost

involved with forensic accreditation by developing a catalogue of approved capabilities and techniques that have FSR endorsement.

- The project will help optimise quality, quality management and accreditation processes by helping forces to meet all their ISO17025 and ISO17020 accreditation standards by 2020 – a key early focus of this project will be to help forces to meet their ISO17025 accreditation standards since the deadline for meeting these was October 2017. The project will then focus upon helping forces to meet their ISO17020 accreditation standards, the deadline for which is October 2020, and creating a catalogue of capabilities and techniques that have FSR endorsement.
- Following the achievement of the ISO standards there is an obligation on the forces to demonstrate continuous improvement in order to maintain the accreditation which TF can support as part of the development of the national approach and roadmap.
- The project will be informed and validated by stakeholder collaboration by working closely with other relevant national programmes, participating police forces, FSPs and the FSR to ensure that its outputs are appropriately informed and validated.
- The project will align with and enable wider police transformation by aligning itself closely with the DII Programme.

Developing and Inspiring People:

- The project will create the digital forensics input for a development programme, aligned to the core values of UK policing, that inspires and nurtures current and future staff.
- The project will create the digital forensics input for an accredited organisational learning, training and competency framework, so that all police forensic personnel are within a Professional Services and Codes of Practice Framework by 2020.
- The project, by constituting a specific area of expertise and theme for discussion and development, will contribute to the creation and development of a “People Forum” to promote regular, frequent, two-way dialogue between the programme and practitioners / frontline operational staff.
- The project will help to embed a culture of continuous improvement by developing a catalogue of endorsed capabilities and techniques; and working with the newly created “People Forum” (see above) to keep it dynamic and up-to-date.
- The project will, through its input into the TF development programme and accredited organisational learning, training and competency framework, support scientific support units and their forensic practitioners in achieving the skills balance required between traditional and digital forensics.

Ensuring Long-Term Sustainability

- The project will pursue opportunities for rationalisation and sharing of specialist capabilities, including the integration of traditional and digital forensic services between now and 2025, where this is in the interests of resilience and value for money and does not weaken local accountability – a key component of this project will be an analysis of the types and volumes of digital forensic capabilities required (by 2019) and an evaluation of how they would best be provided as part of the broader TF landscape and programme.
- The project, owing to the fast-moving nature of digital forensics, will draw extensively upon the expertise of public, private and academic partnerships and, by doing so, maximise opportunities for learning, innovation, continuous improvement and sustainable progress against a common purpose.
- The project, owing to the rapid pace of development in digital technologies and the number of “Original Equipment Manufacturers” (OEMs) involved in the market, will seek (by 2020) to exploit current, future and emerging technology and identify suitable procurement channels / broker appropriate arrangements to access specialist / non-standard services.
- The project will deliver additional value from information and intelligence through increased refinement, sharing, storage, management and analysis of data, supported by appropriate

automation tools and management and business information systems – digital evidence is, by its nature, likely to be distributed across vast networks and the acquisition, analysis and attribution of evidence across these networks provides huge amounts of information and intelligence about criminal activity; consequently a key component of this project will be focused upon maximising opportunities for all police forces to leverage the information and intelligence resulting from digital forensics investigations.

- The project will play a key role in continually reviewing and creating clear, agreed and appropriate requirements to help inform and develop the forensic science market (internal and external to policing) by creating a Technology Readiness Level (TRL) roadmap and catalogue for digital forensics capabilities.
- The project will influence, direct and optimise Research and Development activity by creating a 10-Year Technology Readiness Level (TRL) roadmap and a funding pipeline for research and development, and by managing the dynamic and timely addition of new capabilities to the catalogue of endorsed digital forensics capabilities and techniques being put in place by this project.

2.5 The Current Digital Forensics Landscape

Scope and Demand for Digital Forensic Capabilities

The scope of digital forensics is very broad and, for the purposes of this business case, is defined as "the acquisition, preservation, analysis and presentation of digital data for evidential use in the criminal justice system".

The global Digital Forensics market is typically segmented into 5 main categories and policing needs to be able to access expertise in all these areas:

- computer forensics
- network forensics
- cloud forensics
- mobile device forensics and
- database forensics.

Moreover, policing needs to be able to bring these capabilities to bear across all crime types. Indeed, a recent analysis of crimes reported to Hampshire Constabulary over a sample 2-week period found that every single crime investigation had some form of digital element and this is increasingly the case with criminal investigations across the United Kingdom. The digital element might involve analysis of a suspect's or victim's phone for checking a person's stated whereabouts or record of events. It might involve the analysis of digital evidence recorded by a member of the public or CCTV footage. It might involve analysis of computers, routers, satellite navigation systems or indeed vehicle telemetry systems.

Digital forensics is therefore now the most commonly needed forensic discipline and is witnessing significant increases in demand. Home Office forecasts suggest that the demand for digital forensics will increase by 229 per cent between 2017 and 2020 alone.

It is also a particularly strong form of evidence and one that has a significant impact upon both criminal justice outcomes and their efficiency. 90% of people arrested for child sexual exploitation offences, for example, plead guilty once the initial digital forensics evidence has been presented to them.

Volumes, Spending and Current Organisation of Capabilities

In 2015-16 police forces in England, Wales and Northern Ireland, including the British Transport Police and the *S23(1)*, spent an estimated £74 million on digital forensics and examined approximately 200,000 digital devices; these figures are estimated to be rising by approximately 29% each year. The Transforming Forensics Outline Business Case, prepared in March 2017, estimated that, without a fundamental change in operating model, the cost of digital forensics could reach £162 million per annum by 2022-23.

Police forces across the United Kingdom all have some level of in-house digital forensics capability and most have tended to rely upon local in-house resources to undertake their core caseloads, whilst reserving external support from private sector providers to deal with demand unable to be met locally. The current split between in-house and external provision is understood to be approximately 80% and 20% respectively, but with the percentage requiring external support growing as police forces try to avoid having significant backlogs. In-house capabilities are either delivered by police forces individually or in small collaborative groups.

In addition, digital forensic capabilities are often provided by different parts of a police force. In some cases, digital forensics is the preserve of Hi-tech Crime Units (HTCUs), which normally form part of police forces' intelligence functions. In other cases, digital forensics is part of Scientific Support Units, which are then responsible for all forensic capabilities. In some cases, traditional and digital forensics report to the same line of a police force's senior management team; in others they do not. There are also a number of pockets of digital forensic activity in areas such as Cyber and Child Sexual exploitation, that currently fall outside of any forensic science governance.

External support is provided to police forces through different contracts, again either procured individually or in collaborative groups. There are currently 2 significant collaborative contracts in place for digital forensics. The first is the one put in place by the South West Forensics Hi-tech Crime Unit, which is open to 19 forces in England and Wales plus the Police Service for Northern Ireland. The second is the one put in place by the Metropolitan Police Service, which is open to all UK forces. The main external providers in this field include companies like MASS, CCL, Sytech and IntaForensics.

Good practice is shared between forces both informally and through the auspices of the NPCC Lead for Digital Forensics and the Digital Forensics Portfolio Board. There is general acceptance and buy-in to a "Triage Model", illustrated below and endorsed by the NPCC's Digital Forensics Portfolio Board, and many forces have either already adopted or are in the process of adopting such a model. Similarly, the creation of a Forensic Marketplace Strategy Group is helping to rationalise procurement activity. Police forces can however procure and organise their digital forensic services in whatever way they believe will meet their operational needs most effectively.

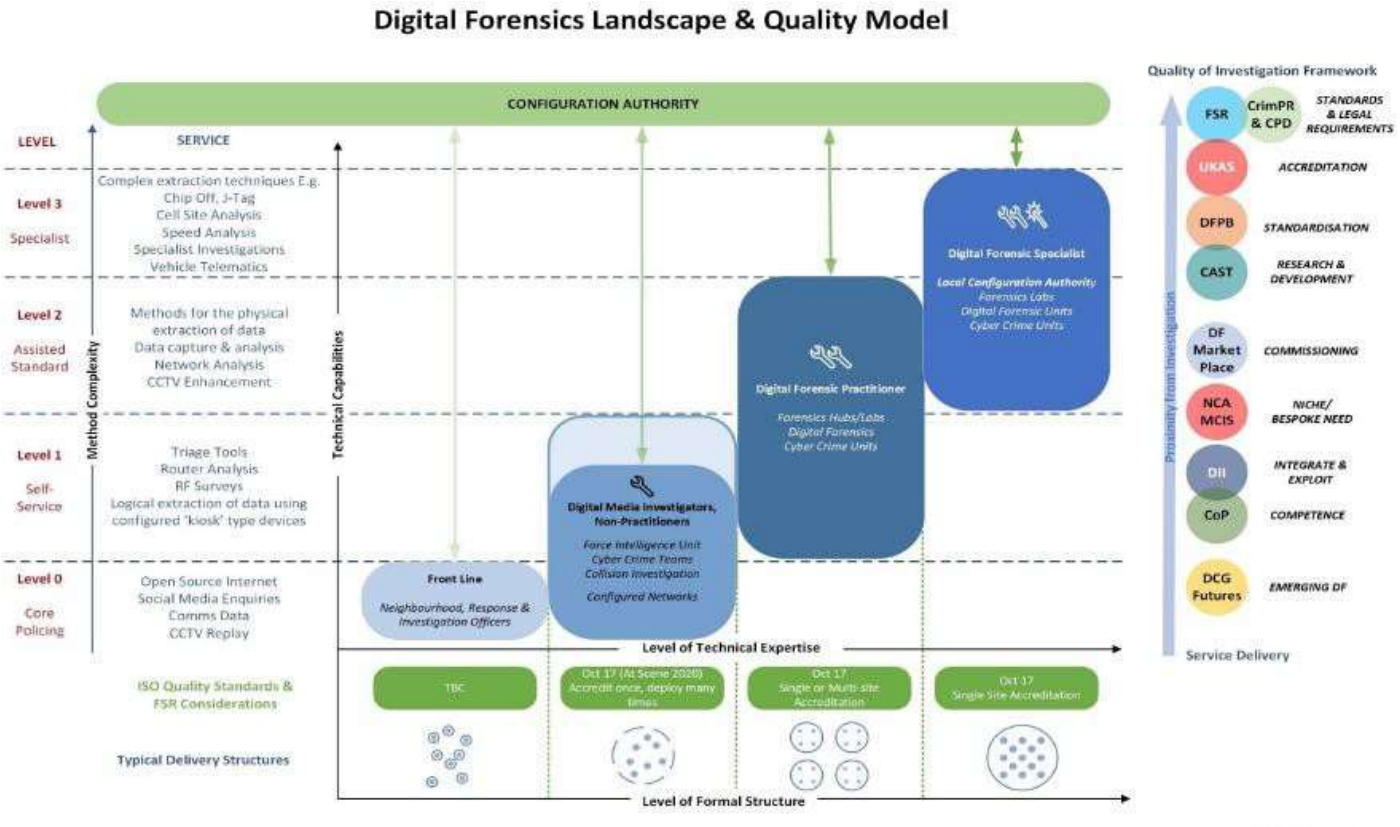


Figure 2 – Digital Forensics Landscape and Quality Model (NPCC and Digital Forensics Board)

Quality Standards and Accreditation

All forensic capabilities need to meet quality standards prescribed by the Forensic Science Regulator and organisations providing them need to be accredited to do so by the United Kingdom Accreditation Service (UKAS). Accreditation standards cover both laboratory-based processes (ISO17025) and scene-based processes (ISO17020). The prescribed timetable for meeting the accreditation standards associated with digital forensics are set out below:

Activity	Accreditation Deadline
Imaging of hard drives and removable media	October 2017
Screening or recovery of data from a device using an "off the shelf" tool for factual reporting	October 2017
Extraction and analysis of data from digital media including remote storage	October 2017
Network capture and analysis	TBC - October 2018
Capture and analysis of social media and open source data	TBC
Cell-site analysis and communications data	TBC
Scene-based recovery and analysis	October 2020

There are currently circa 60 policing and law enforcement organisations that provide digital forensic capabilities: namely the 43 police forces in England and Wales, Police Scotland, the Police Service for Northern Ireland, the British Transport Police, various Counter Terrorism Units and agencies such as HMRC. Most forces missed the October 2017 deadlines for accreditation, with the small number who did make it, having to make some very serious decisions on resourcing, due to the significant overhead in terms of both cost and time that obtaining and then maintaining accreditation entails. Forces are all operating as their own legal entities, so are having to approach the same or similar issues as neighbouring forces, without the efficiencies that a more national approach would bring. This is expending an enormous amount of time and cost during severe reductions in policing budgets. Over half of policing and law enforcement organisations are still not accredited to the standards prescribed by the Forensic Science Regulator to be in place by October 2017.

Technology Changes and Research and Development

Changes in the digital forensics market are driven by consumer demand for ever more powerful capabilities. This makes Original Equipment Manufacturers (OEMs) a powerful resource. It also means that research and development is currently very much supplier-led.

New capabilities are then offered to police forces, often through direct targeting of Digital Media Investigators or individuals within Hi-tech Crime Units within each force. Forensic science practitioners and their organisations, working in relative isolation, do not have the leverage required to engage with OEMs to negotiate appropriate access to data and technical support e.g. encryption.

As a result, direct Police Service direction or influence over R&D in digital forensics is currently limited and police forces usually find themselves having to "play catch-up" with the capabilities employed by the more sophisticated elements of the criminal fraternity.

2.6 Business Needs - The Case for a Targeted TF Digital Forensics Project

There are 6 main reasons why there is a need for a specific Digital Forensics project within the broader Transforming Forensics Programme.

The first is that the current arrangements for digital forensics across policing are fragmented, sub-optimal, carry inherent risk and are out of alignment with both Policing Vision 2025 and the Home Office's Forensic Science Strategy.

As set out in section 2.5, the current digital forensic landscape is both fragmented and inconsistent in its operation and service delivery. This has created an environment of both process and technical divergence across the operating landscape and has led to a series of sub-optimal outcomes, including:

- digital forensic capabilities in UK policing lagging significantly behind those of other countries, especially in the Netherlands, Germany and the United States;
- approximately half of UK law enforcement organisations failing to meet their accreditation standards by the deadlines set by the FSR - those unaccredited present a risk to both the quality and the credibility of the capability within forces;
- significant backlogs developing, where police forces are either unable to investigate the digital aspects of a crime at all or can only do so after unacceptable delays;
- digital forensics capabilities and the resulting evidence/ intelligence being confined to individual police forces and departments within those police forces through Hi-tech Crime Units often being isolated from both their traditional forensic science colleagues and their force IT departments;
- digital forensic science training being very expensive;
- existing governance and boards not managing to channel their collective energies across the myriad of technologies considered as digital forensics, resulting in fragmented services, a fragmented supply chain, piecemeal change, and low levels of collaboration, cost sharing, knowledge sharing and indeed intelligence sharing from digital forensics investigations;
- funding and energy for change being distributed across the digital forensic landscape, making it difficult to make the large step changes in capability or service quality that are needed;
- police forces adopting a "follow my leader" approach as different capabilities and standards are copied from one force to another, without necessarily stepping back and reappraising requirements from a holistic police service perspective;
- UK policing being unable to exert significant influence over research and development efforts;
- UK policing being unable to engage with Original Equipment Manufacturers (OEMs) to negotiate appropriate access to data and technical support;
- UK policing having no national technical authority for digital forensics;
- UK policing having no clear picture of planned digital forensics activity across the country.

In summary, existing arrangements are holding back innovation, leading to costly, inefficient and risk-laden operations, and leaving market power with suppliers rather than customers.

The second is that the pace of change in digital forensics and the growing demand for its capabilities are too great for police forces to tackle individually.

Police forces have made significant progress in bolstering their digital forensics capabilities and have responded well to some of the challenges posed by the proliferation of digital technologies. The "4 Level Triage" Model illustrated in section 2.5, for example, has led to significant increases in the volume of devices able to be analysed, as well as significant decreases in the average costs of each examination. The Metropolitan Police Service, for example, has, over the last 5 years, achieved an 84% reduction in average turnaround times and a 54% reduction in average examination costs from introducing this new model, whilst accommodating a 65% increase in throughput. Other forces have achieved similar levels of improvement.

Nevertheless, police forces are struggling and will continue to struggle to keep up with demand. This is because firstly, and through continual advances in information technology and service capabilities, digital forensics is the fastest growing and fastest changing area of forensic science. 5G telecommunications networks will, for example, be able to carry data 86 times faster than current 4G networks. And by 2020 there are expected to be 5 billion internet users and 100 billion internet-connected devices worldwide (the Internet of Things). Secondly, overall levels of crime, and those reported to the police, are increasing. In the year to the end of June 2017, there were an estimated 10.8 million[2] incidents of crime in England and Wales, of which 5.2 million[3] were reported to the police. This level of reporting represented a 13% increase on 2016 and followed similar increases of 5% in 2015 and 7% in 2016. Furthermore, digitally enabled crime is conservatively estimated as increasing at a rate of 29% per year. The estimated cost of cybercrime in the UK in 2015 was £27 billion. In other words, policing is having to deal with increasing levels of reported crime, almost all of which will have some form of digital footprint and where the numbers of devices involved, and the associated digital storage, are rapidly increasing. Home Office forecasts suggest demand for digital forensics will increase by 229% between 2017 and 2020 alone. Thirdly, responding to demand creates its own demand. Providing digital data extraction kiosks, for example, encourages more people to use them, thereby generating additional demand for their services.

And then there is of course the current increased threat of terrorism and the counter-terrorism activity, which relies increasingly upon the analysis of digital activity and material.

The third is that the nature of digital technology, the ways in which it is supported and the standards against which it is measured are changing, necessitating a different approach from policing and providing new opportunities.

Digital forensics has traditionally involved examining a forensic image taken from a seized device because until relatively recently the norm has been for data to be stored on devices. The advent of cloud computing has changed all this, with the norm now becoming that data is stored across vast storage area networks, located anywhere in the world and accessible from anywhere in the world. The traditional digital forensics operating model is therefore needing to change, with techniques such as big data analysis becoming more commonly required. HMRC, for example, recently needed to image and analyse 1 petabyte of data for a single banking-related investigation.

At the same time, criminals are exploiting technology, encryption and the tools to preserve anonymity online, often more quickly than law enforcement can bring new techniques to bear. Similarly, “educated” computer criminals are now using a range of anti-forensic techniques and tools, including cryptography, disk cleaning and file wiping utilities that focus upon destroying and altering data, thereby obfuscating the forensic trail.

Policing therefore needs to develop effective new forensic tactics and capabilities to help detect, identify and ultimately bring offenders to justice. Attempting to do this in a piecemeal way, with police forces trying to tackle these challenges individually, is unlikely to succeed.

With new techniques, of course, come new accreditation requirements and this is a particular challenge for digital forensics due to the pace of change. There is currently conflict between the relatively static nature of the FSR’s ISO17025 and subsequent force standard operating procedures (SOPs) and the pace of digital development. Policing therefore needs to find a way to work with the FSR to achieve appropriate agility in SOP development, so that digital forensics techniques can keep up with the capabilities deployed

[2] Office for National Statistics – Crime in England and Wales year ending June 2017.

[3] Only 5.2 million crimes were reported to police because not only do some crimes go unreported but a significant percentage (83%) of fraud-related crimes e.g. bank and credit card fraud are reported to and addressed directly by customers’ financial institutions. 5 million of the 10.8 million crimes related to fraud and computer misuse, with the remaining 5.8 million relating to the more “traditional” crime types such as violent crime, theft, burglary and criminal damage.

by criminals. Otherwise, the criminals will continue to exploit the changing technologies available to them and the gap between police capability and criminal activity will widen further. Again, attempting to work with the FSR in a piecemeal way, with police forces trying to tackle these challenges individually, is unlikely to succeed.

Finally, there are techniques available that, with the right amount and focus of investment, could potentially revolutionise the way that digital forensics is able to piece together information. Block chain technologies, which were originally designed to help complex supply chain management over multiple international borders, are the technologies used for cryptocurrencies like Bitcoin. They are also used to facilitate a lot of the clandestine activity found on the Dark Web. However, the development and deployment of "permission block chain solutions" could enable forensic examiners to understand the sequential chain of events faster and with more precision than currently. Similarly, the type of automation and machine intelligence that is currently used within the Child Abuse Image Database (CAID) to identify existing image matches and help categorise new images offers huge potential for speed and quality improvements across a broad range of digital forensics disciplines. Furthermore, technology is being developed that will provide end to end case management with machine learning and elastic search. This is exactly what digital forensics needs so that it can automate and orchestrate digital forensic processes, freeing up examiners to work on the more contentious areas of interpretation and review etc. The advantages of police forces working together to achieve such outcomes are clear.

The fourth is that the importance of digital technology, and indeed the digitisation of many traditional forensic processes and information, requires much more integration of digital and traditional forensics capabilities than was previously required.

Digital evidence is playing an increasingly significant role in criminal investigations. Similarly, digital capture and transmission of traditional forensic processes, such as fingerprints, and the digital storage of forensic evidence alongside other case information are bringing digital and traditional forensics closer together. However, since digital technology is a relatively new development, the fields of digital media investigation and crime scene examination have tended to be undertaken by separate teams within each police force. This approach has significant limitations, particularly when it comes to analysis of the initial crime scene. A crime scene investigator (CSI) will traditionally secure fingerprint, DNA and other evidence. In a digital world, the police force will often need to secure evidence from any digital devices at the crime scene, including the Wi-Fi router. Sometimes this will also need to be undertaken in "live time" since vital evidence could be lost if the router, for example, is either left too long or even switched off. Achieving an integrated approach between digital and traditional forensics, right from the point of a crime being reported, is therefore now paramount.

In addition, the balance between digital and traditional forensics is changing. Home Office estimates suggest that the demand for traditional forensics will decline by 13% between 2017 and 2020, whilst the demand for digital forensics will increase by 229%.

This raises an interesting set of challenges and points to the need to help re-skill and augment the police forensics workforce so that it can deal with both traditional and digital forensics in an integrated way.

The fifth is that police forces have significant data protection and disclosure obligations, which are currently difficult to meet, either reliably or cost effectively, and will become more demanding when the General Data Protection Regulation (GDPR) comes into force on 25th May 2018.

Police forces have significant data protection and disclosure obligations under both existing data protection legislation and the Criminal Procedure and Investigations Act (CPIA), which places a duty on police forces to review and disclose evidence that might help the defence. Several recent high-profile cases, where rape or sexual assault cases have been abandoned at the last minute, have shown that this is not always happening. The General Data Protection Regulation (GDPR), which comes into force on 25th May 2018, increases the duties upon police forces and gives data subjects the right for information relating to them to be rectified or erased ("the right to be forgotten") in appropriate circumstances. The Regulation also gives data subjects the right to know what information is held about them, how it is

processed, retention periods and any transfers to other parties. Evidence gathered through digital forensic science capabilities is often currently isolated from other information held by a police force and could therefore either be easily overlooked or be more administratively costly to retrieve.

The sixth is that without a bespoke Digital Forensics project, the potential benefits and opportunities associated with the national Digital Intelligence and Investigation (DII) Programme, and indeed the Home Office Biometrics (HOB) Programme, are unlikely to be maximised.

Significant investment is currently being made in both the DII and HOB programmes. The former is seeking to create a consistent Target Operating Model (TOM) for digital intelligence and investigations and to support forces in achieving it. The latter is developing Biometric services, including facial recognition, which will play an important role in analysis of photographic and CCTV evidence recovered by police forces.

Neither of the above will be able to maximise their benefits without the digital forensic capabilities needed to underpin them and forensics becoming an integral part of investigations rather than being viewed as an "add-on" capability. Nor will digital forensics capabilities be able to fulfil their potential without alignment to an effective investigation model or an effective national facial recognition capability. A bespoke Digital Forensics project is therefore needed to help maximise the benefits of all 3 areas.

Allied to this, and to the development of cloud computing and big data analytics etc., is the need for effective networking of digital forensic capabilities. Crime is not constrained by geography and neither are police investigations. The need to be able to share forensic evidence and its related intelligence both nationally and internationally cannot be underestimated. There is a real opportunity for digital forensics to assist policing in preventing criminality through greater use of forensic intelligence and to identify criminals earlier, thereby bringing swifter justice for victims and preventing further victims in the future. Being able to share specialist skills will also be key. Both aspects require fundamental changes to current capabilities and operating models.

Finally, the challenges facing digital investigations and digital forensics require solutions at a technical, legal and policy level because of the significant ethical issues surrounding the need for the state to be able to protect its citizens, whilst respecting personal privacy. By having a Digital Forensics project closely aligned to other programmes, these sensitive issues and debates can be progressed in a coherent and cohesive manner.

These drivers for change show that there is a clear and pressing business need to develop the digital forensics landscape over the coming years and find new ways of operating, which will both meet the upcoming challenges and address the shortfalls in existing arrangements.

2.7 Proposed Business Scope and Key Service Requirements

To address the drivers for change set out in section 2.6, the Transforming Forensics Programme has identified the following as key business needs:

- to develop a collaborative programme approach, both with police forces and other national programmes, that enables the existing services to help define policing's longer-term capability requirements and to self-reform;
- to deliver a sustainable, consistent, integrated, quality assured network of digital forensic capabilities;
- to develop a "people" approach that grows the right skills, behaviours and standards necessary to deliver high quality digital forensic services;
- to deliver long-term sustainability of digital forensic services with increased levels and pace of innovation.

Given the complexity of digital forensics, the fragmented marketplace (both internal and external to policing) and the rapidly changing landscape, the scale of the Digital Forensics challenge should not be under-estimated. Delivering a sustainable, consistent, integrated, quality assured network of digital

forensic capabilities will take time and it is imperative that this project invests its energy and funding into activities and outputs that will make most impact. Consequently, the TF Digital Forensics project is advocating a staged approach, aimed at building confidence and consensus amongst its stakeholders, and supporting the development of capability, rather than undertaking large scale operational delivery or any significant capital investment in technology or infrastructure at this stage.

The project's activity will therefore initially focus upon:

- Leadership and governance, including the establishment of appropriate governance boards, and the development and management of a 'portfolio-level' plan for Digital Forensic Science;
- Establishing a 'Digital Advisory' capability focused on supporting digital forensics and developing and executing longer-term strategies to deliver the TF programme's objectives;
- Developing innovative, longer-term funding models and roadmaps to increase the pace of innovation and change.

Table 1 - Project Deliverables / Objectives below sets out the scope of the project's activities and the related deliverables / objectives they will achieve. It is organised into 3 strategic capability strands (National Capability Management, Service Provision and Quality Working) set out in the broader Transforming Forensics Programme Business Case.

Table 1 - Project Activities and Related Deliverables / Objectives

Strategic Capability Strand	Activity	Related Deliverables / Objectives
National Capability Management *Delivery Timescale – by September 2018*	Building upon existing Boards and working closely with the DII programme, establish a national authority for Digital Forensics with leadership over technical requirements, quality and processes	Creation of the Digital Forensics standard setting and online document / material library aspects of the Forensic Capability Network, together with the national authority to create, endorse, maintain and manage a catalogue of approved capabilities and techniques
National Capability Management *Delivery Timescale – by September 2018*	Construct a detailed baseline of force digital forensic capabilities and initiatives, including contracts, procurement and change projects, and make equivalent assessments of demand	A comprehensive understanding of the digital forensics landscape and current pinch points etc. in order, over time, to align demand and supply as part of an effective network of digital forensic capabilities
National Capability Management *Delivery Timescale – by January 2019*	Forge effective public / private / academia partnership to undertake research into future capabilities (emerging and potential) to inform future focus and investment	Creation of a 10-Year Technology Readiness Level Roadmap and associated funding and development pipeline
National Capability Management *Delivery Timescale – by January 2019*	Produce recommendations, supported by a business case, for the creation of a resilient and future-proofed network of digital forensic capabilities, forming part of an integrated forensics capability and incorporating	Blueprint and business case for the digital forensics elements of a broader Forensic Capability Network

Strategic Capability Strand	Activity	Related Deliverables / Objectives
	networking arrangements for evidence management and sharing of intelligence, aligned to the agreed service operating model (see below)	
National Capability Management *Delivery Timescale – by January 2019*	Design a new funding model to support a sustainable, consistent, integrated, quality assured network of digital forensic capabilities	Creation of the Digital Forensics elements of a Forensic Capability Network that is resilient; incorporates up-to-date capabilities and techniques; provides access to all at a cost that is affordable and fair; matches supply efficiently with demand; and is not reliant upon future "Police Transformation Fund" or equivalent grant support
Service Provision *Delivery Timescale – by June 2018*	Establish a 'Digital Advisory' capability covering the appropriate breadth and depth of digital forensics expertise to support forces in meeting their 'digital forensic' challenges	Achieving a collaborative approach; demonstrating programme value; ensuring that all forces can deploy required capabilities and techniques
Service Provision *Delivery Timescale – by November 2018*	Create, along with the DII Programme, a service operating model for a broad range of investigative / forensics scenarios, providing clarity on capabilities and techniques and how best to deploy them	Forces able to undertake more effective investigations and reduce the direct cost per case outcome by at least 25%
Service Provision *Delivery Timescale – by December 2018*	Create effective links with OEMs to gain access to appropriate data and technical support	OEMs more conscious of digital forensic needs and able to support policing requirements
Service Provision *Delivery Timescale – by mid-2019*	Work with forces and other stakeholders to create a catalogue of approved / endorsed capabilities and techniques	National alignment and cohesion through an approved catalogue of capabilities and techniques
Service Provision *Delivery Timescale – by mid-2019*	Work with forces to address current shortfalls in digital forensic support skills, notably the availability of technicians to support frontline digital forensic services	Creation of more integrated forensic services that are better able to support the range of demands being placed upon them
Service Provision *Delivery Timescale – by mid-*	Work with forces, the Forensic Science Marketplace Group and	Achieving efficient access for all to the approved catalogue of

Strategic Capability Strand	Activity	Related Deliverables / Objectives
2019	potentially the Police ICT Company to help procure new capabilities / rationalise existing capabilities	capabilities and techniques
Quality Working *Delivery Timescale – during 2018 and 2019*	Support forces with short-term ISO17025 and medium-term ISO17020 accreditation activities (part of the related Standards and Accreditation Project)	Achieving a collaborative approach; demonstrating programme value; ensuring that all forces meet FSR quality standards and achieving an overall reduction in accreditation time and cost
Quality Working *Delivery Timescale – by mid-2019*	Define and construct the Digital Forensics elements of the TF learning and development programme	Forensic staff all benefit from an accredited learning and development programme; are part of a Professional Services and Codes of Practice Framework by 2020 and are part of an integrated future-proofed digital forensics capability by 2025
Quality Working *Delivery Timescale – during 2018 and 2019*	Represent forces and work with the FSR to produce quality standards, operating models and codes of conduct, which can keep pace with digital forensics	Forces able to meet ISO17025 and ISO17020 accreditation requirements, whilst being able to keep up with the pace of change in digital forensics

2.8 Main Benefits

The Digital Forensics project is expected to deliver very significant financial and non-financial benefits.

The expected financial benefits are still to be quantified and will depend upon both the information collected as part of the forthcoming baselining exercise and the precise nature of project activities. However, based upon a combination of the analysis undertaken for the related Fingerprint and Standards and Accreditation business cases, the Transforming Forensics Outline Business Case (March 2017) and the experience of the MPS, as set out in section 2.6, the project believes that annual savings of at least 20% could be achieved by adopting a similar "Forensic Capability Network" approach, investing in greater automation capabilities and improving the overall operating model. With spending on digital forensic science soon expected to exceed £100 million per annum, the Digital Forensics project will be targeting ongoing financial savings of at least £20 million per annum.

The expected non-financial benefits of the project include:

Table 2 – Benefits

Expected Benefit	Estimated Delivery
Cohesive strategic direction and a bespoke science and technology roadmap, ensuring that services are up-to-date and aligned with other national programmes	From 2018 onwards
Nationally defined and agreed digital forensic specifications and standards, which will greatly benefit accreditation, procurement and integration	From 2019 onwards

Expected Benefit	Estimated Delivery
with other departmental roadmaps (IT and Estates etc.), as well as the interface between forensics, investigations and the criminal justice system (prosecution and defence)	
Reduced risk through cohesive governance and management of forensic provision	Blueprint scheduled for delivery during 2019, with new landscape by 2025 at the latest
Long-term sustainability of digital forensic services, with capabilities closely aligned with demand and access to expertise and an enhanced skill base when and where it is needed	Blueprint scheduled for delivery during 2019, with new landscape by 2025 at the latest
Better value for money by having an ecosystem of expertise, meaning that forces do not all have to maintain a cadre of the same specialist and therefore expensive posts	Blueprint scheduled for delivery during 2019, with new landscape by 2025 at the latest
Better value for money by achieving economies of scale and a less fragmented digital forensic service and supply chain, as policing speaks with one voice in commercial negotiations and with regards to Research and Development (R&D) priorities	From 2019 onwards
Increased productivity for policing, enabled by consistent and transparent performance management and the use of clear and transparent service levels against nationally agreed outputs, linked to policing outcomes	From 2019 onwards
Integration of digital and traditional forensic capabilities, with the ability to cross-fertilise skills across the workforce	From 2019 onwards
Future proofed science and technology offering best of breed services, backed up by a robust R&D capability and an agreed development roadmap	From 2019 onwards
More effective engagement with Original Equipment Manufacturers (OEMs), providing appropriate access to data and technical support	From 2018 onwards

2.9 Main Risks

The main risks, together with their associated mitigations, are set out in the table below.

Table 3 – Risks

Risk	Mitigation
The linked “Standards and Accreditation” project within the Transforming Forensics Programme does not proceed due to lack of funding.	A decision will need to be made regarding the composition of the Digital Forensics project and whether ISO accreditation support should be progressed for Digital Forensics in isolation.

Risk	Mitigation
The Transforming Forensics Programme does not attract sufficient Police Transformation Funding to support a meaningful Digital Forensics project.	PCCs and police forces could be approached directly for funding, supported by this business case.
There is insufficient support from participating forces to help deliver the project's intended deliverables in a timely and effective manner.	There will be a strong focus on communications and building a programme delivery team that includes significant contributions and representation from participating forces.
The project is unable to engage satisfactorily with the complex Digital Forensics marketplace.	Further help could potentially be enlisted from organisations like the Association of Forensic Science Providers, the Chartered Society of Forensic Sciences or TechUK.
The project is poorly aligned with the DII Programme and causes overlap or conflict.	An initial inter-programme (Transforming Forensics and DII) workshop has been held and regular liaison between the two programmes will be the norm throughout the DF project's lifetime.
The project struggles to create a 10-Year Technology Readiness Level roadmap because of the fast-paced nature of digital forensics.	Although the pace of technological development is particularly fast, there are some areas of predictability. If needed, the timeframe of the TRL roadmap will be adjusted.
Individual police forces are unable to wait for the creation of a "TF - endorsed" catalogue of capabilities and invest in a piecemeal way.	The project will adopt a pragmatic approach and create its "endorsed" catalogue in stages, focusing first upon areas that are of immediate benefit to forces.
The TF programme is unable to agree an appropriate funding model to sustain the maintenance of the project's intended deliverables beyond March 2020.	Significant effort will be focused upon devising an appropriate funding model in the early stages of the project.

2.10 Constraints

Constraints are the internal parameters that have been established at the outset of the project. These have been identified as follows.

Table 4 – Constraints

Title	Description	Impact
Capacity	The Transforming Forensics programme team is small and is still comparatively light on digital expertise	The Digital Forensics project will need to work closely with the DII Programme and with digital forensic experts across law enforcement to provide the necessary leadership and momentum to make a lasting impact.
Capacity	The project needs to be manageable	The project will need to be designed well,

Title	Description	Impact
	alongside other local police force change activities.	agreed with all participants in advance and well managed throughout. It will also need to dovetail with other national and local initiatives, especially those also supported by the Police Transformation Fund e.g. the DII Programme.
Regulatory Compliance	Only approximately one half of policing bodies have complied with current FSR timelines for ISO17025 accreditation of digital forensic capabilities.	The project will need to maintain an early focus on helping forces to meet current Digital Forensics accreditation standards.
Regulatory Compliance	Public Contracts regulations may result in the procurement / acquisition of new capabilities taking longer than desired.	The project will need to identify appropriate procurement routes, which comply with the 2015 Public Contracts Regulations but achieve the desired outcomes in the quickest possible time.
Scope	Fully addressing the Digital forensics challenges will require funding and time beyond the existing Police Transformation Fund (PTF) window	The project scope will need to be tightly defined to maximise the benefits achievable from the funding and time available.
Funding	There is currently no funding set aside for a Digital Forensics project.	The project will require Police Transformation Funding to proceed and will need to be managed within its agreed funding limits.
Timing	Police Transformation Funding, if granted, will only be available until 31 March 2020.	The project will need to have concluded by the end of March 2020.

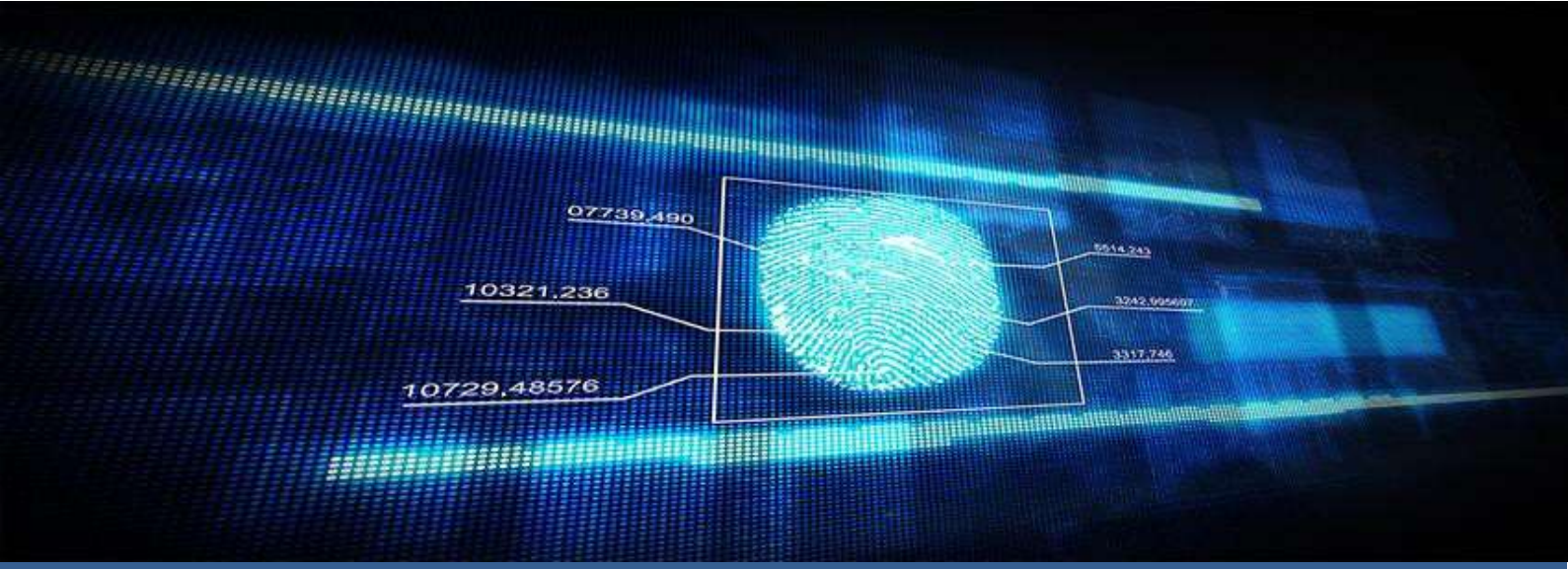
2.11 Dependencies

Dependencies are the external influences on the project – namely things which must be in place to make a success of this investment.

The Digital Forensics project is subject to the following dependencies, which will be carefully monitored and managed throughout the lifespan of the project:

- timely progress being achieved on associated TF projects, particularly "Standards and Accreditation" and the wider Forensic Services Operating Model;
- timely progress being achieved by the DII Programme with regards to the overarching Digital Intelligence and Investigations Target Operating Model and appropriate linkages being made between the TF and DII programmes;
- timely progress being achieved by the Digital First Programme, which along with DII and Digital Public Contact as part of the broader Digital Policing Programme, is exploring solutions to the broader challenges of evidential capture, storage, management and movement across the Criminal Justice System (CJS);
- sufficient police force and practitioner involvement in testing and agreeing the digital forensic capabilities to be included within the new catalogue of "endorsed" capabilities and techniques;

- sufficient engagement with and expertise from Counter Terrorism;
- sufficient engagement with digital forensics suppliers and academia etc. to be able to create a reliable Technology Readiness Level roadmap;
- the support of the Forensic Science Regulator;
- the ability and capacity to procure, within the timeframes available, the necessary technology capabilities or components needed to achieve the project's intended deliverables;
- availability of appropriate independent evaluation team resources to ensure that findings are robust and peer-reviewed;
- to a lesser extent, in the period up to March 2020, the availability of the new facial recognition capabilities expected to be provided by the Home Office Biometrics (HOB) Programme.



3. The Economic Case

3.1 Introduction

This section of the Strategic Outline Case documents the process undertaken to determine the most economically advantageous option for progressing the current stage of the Digital Forensics Project. The Economic Case is not at this stage a full options appraisal. A full options appraisal will be undertaken at Outline Business Case Stage, which is currently scheduled for the end of December 2018.

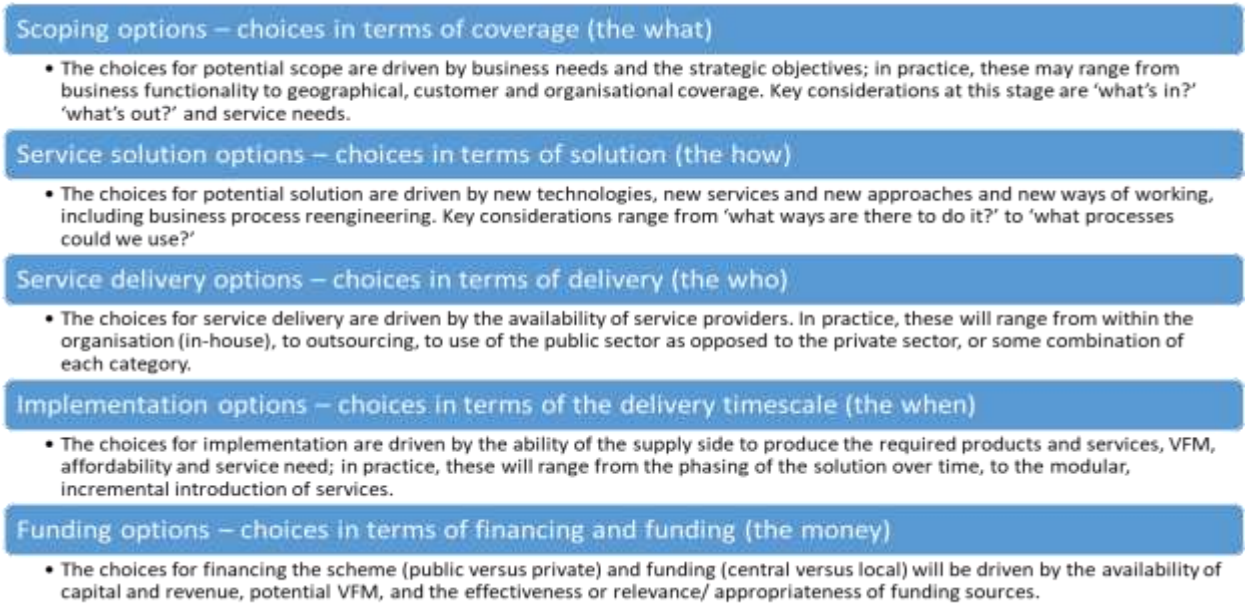
3.2 Critical Success Factors

The critical success factors (CSFs) are the criteria against which the project will judge its success, and which have been used alongside other factors when assessing long and short-listed options. The project's CSFs are:

1. **Strategic fit** - how well the option fits with key strategies including: Policing Vision 2025, the Home Office's Forensic Science Strategy and the Transforming Forensics Programme's own Vision, Mission, Objectives, Strategies and Tactics (VMOST) – full details set out in the Strategic Case;
2. **Meeting business needs** – how well the option satisfies existing and future business needs;
3. **Benefits optimisation** – how well the option optimises the potential return on investment (business outcomes and benefits) and assists in improving Value for Money (VfM), generating either additional revenue or capacity to meet demand;
4. **Affordability** – how affordable the option is to police forces, based upon the capital and revenue consequences associated with the proposed investment;
5. **Achievability** – how achievable the option is, in the light of available timescales and market capacity / capability etc.

3.3 The Long-listed Options

In line with good practice, the long list of options was generated through a systematic examination of the choices the project faces. The choices were identified based on the following considerations.



This approach gave a long-list of 11 options, as set out in the table below.

Table 5 – The Long-List of Options Considered

Option	Description
1	Do nothing and leave forces to develop their own capabilities using existing governance and collaborative structures
2	Establish an in-house / police-led advisory capability with the limited scope of supporting forces with the implementation of the findings of the "Enabling Digital Forensics" Proof of Concept project (extraction of digital data from devices using kiosks) and with their ISO 17025 and ISO 17020 accreditation challenges – effectively those elements already within the scope of the Transforming Forensics Programme
3	Establish an outsourced version of Option 2
4	Establish an in-house / police-led advisory capability with a much broader scope, building upon Option 2 but including all techniques and capabilities involving the acquisition, preservation, analysis and presentation of digital data for evidential use in the criminal justice system
5	Establish an outsourced version of Option 4
6	Establish an in-house delivery service, designed to provide digital forensic science services to police forces across England, Wales and potentially Northern Ireland
7	Establish an outsourced version of Option 6
8	Establish an in-house / police-led advisory capability with the scope of Option 2 but with the additional remit to determine whether there is a business case to deliver the corresponding services to police forces across England, Wales and potentially Northern Ireland
9	Establish an outsourced version of Option 8

10	Establish an in-house / police-led advisory capability with the scope of Option 4 but with the additional remit to determine whether there is a business case to deliver the corresponding services to police forces across England, Wales and potentially Northern Ireland
11	Establish an outsourced version of Option 10

3.4 Short-listed Options

The long-list was quickly reduced to a short-list of 6 options by discounting all outsourced options. The reasons for this were that:

- at present there is not a sufficiently well-defined baseline, or indeed digital forensic science scope, for an outsourcing exercise to be undertaken with any confidence or reliable metrics or performance measures;
- an outsourced approach at this stage is unlikely to secure the levels of engagement and buy-in needed from police forces;
- an outsourced approach at this stage would not help to build internal knowledge and expertise;
- outsourcing at this stage would be at odds with the current police-led approach of the broader TF Programme and would also be at odds with the approach advocated in the TF Programme Business Case for the Forensic Capability Network – namely an "in-house service, using sub-contracts and bought-in services where this is plainly more efficient";
- outsourcing for any delivery options usually comes with significant up-front costs and often involves outsourcing technical design, build and operation to a third party. Given the pace of change in digital forensics and the currently limited knowledge of the policing baseline, such an approach would carry too great a risk at this stage;
- the TF Programme can already deploy an appropriate blend of in-house and external expertise through its Delivery Partner contract.

This approach gave a long-list of 6 options, as set out in the table below.

Table 6 – The Short-Listed Options

Option	Description
1	Do nothing and leave forces to develop their own capabilities using existing governance and collaborative structures
2	Establish an in-house / police-led advisory capability with the limited scope of supporting forces with the implementation of the findings of the "Enabling Digital Forensics" Proof of Concept project (extraction of digital data from devices using kiosks) and with their ISO 17025 and ISO 17020 accreditation challenges – effectively those elements already within the scope of the Transforming Forensics Programme
3	Establish an in-house / police-led advisory capability with a much broader scope, building upon Option 2 but including all techniques and capabilities involving the acquisition, preservation, analysis and presentation of digital data for evidential use in the Criminal Justice System (CJS)
4	Establish an in-house delivery service, designed to provide digital forensic science services to police forces across England, Wales and potentially Northern Ireland

5	Establish an in-house / police-led advisory capability with the scope of Option 2 but with the additional remit to determine whether there is a business case to deliver the corresponding services to police forces across England, Wales and potentially Northern Ireland
6	Establish an in-house / police-led advisory capability with the scope of Option 3 but with the additional remit to determine whether there is a business case to deliver the corresponding services to police forces across England, Wales and potentially Northern Ireland

3.5 Options Analysis Against Critical Success Factors

Each of the shortlisted options was the assessed against the Critical Success Factors set out in section 3.2. The results are shown in the table below.

Table 7 – Analysis Against Critical Success Factors

Critical Success Factor	Option 1 Do Nothing	Option 2 Limited Scope Advisory	Option 3 Broad Scope Advisory	Option 4 Limited Scope Delivery	Option 5 Broad Scope Delivery	Option 6 Broad Scope Advisory and Delivery Business Case
Strategic Fit	Poor – out of line with Policing Vision 2025 since it does nothing to meet the challenges faced by policing as a whole	Limited – in line with Policing Vision 2025 but scope not going to transform the broader digital forensics landscape	Good – in line with Policing Vision 2025 and potential to achieve greater cohesion across the broader digital forensics landscape, working closely with the national DII and Digital First Programmes	Limited – could create some shared specialist capabilities in the shorter term but lacks the benefit of taking a more holistic approach and could create unhelpful barriers between different digital forensics capabilities	Mixed – could create a strong network of specialist capabilities but will not gain the support of forces or PCCs without much greater analysis and a clear picture of the future design	Optimum – as Option 3 but with the potential for future Forensic Capability Network delivery and benefiting from the rigour of a more detailed business case
Meeting Business Needs	Poor – does nothing to meet business needs	Limited – would support accreditation challenges and extraction of digital data but would do nothing for the broader landscape	Good – makes much more sense to take a holistic view of digital forensics rather than focus upon discrete areas with more limited benefit potential	Limited – would not be viable for accreditation. Could be helpful for “kiosk” type digital extraction from devices but many local initiatives already in train	Poor – until further analysis has been undertaken, a service operating model has been agreed with DII and forces and PCCs can see a future design they could support	Optimum – as Option 3 but with the additional information needed to be able to consider a potential rationalisation of some capabilities

Critical Success Factor	Option 1 Do Nothing	Option 2 Limited Scope Advisory	Option 3 Broad Scope Advisory	Option 4 Limited Scope Delivery	Option 5 Broad Scope Delivery	Option 6 Broad Scope Advisory and Delivery Business Case
Benefits Optimisation	Poor – does nothing to optimise benefits	Limited – would support the benefits realisation of the "Standards and Accreditation" project and potentially help to support "kiosk" digital extraction take-up but limited impact across the scope of broader digital forensic science	Good – would be expected to provide much more holistic results by working closely with the DII and Digital First programmes and be able to help optimise benefits across the 3 related programmes	Limited – owing to limited scope and unlikely to engender much buy-in until supported by a comprehensive evaluation of the option and a supporting business case	Poor – without a clear future service operating model design, this option would not currently attract sufficient buy-in to optimise benefits	Good – would deliver the same benefits as Option 3 but with the potential for much greater benefits in the longer term, as well as a much better picture of the current landscape
Affordability	Easy – no investment required	Relatively easy – limited investment required through PTF	Relatively easy – modest investment required through PTF	Difficult – required investment unknown at present but expected to be significant and long-term	Very Difficult – required investment unknown at present but expected to be very significant and long-term	Relatively easy – modest investment required through PTF
Achievability	Easy – requires no effort	Relatively easy - recruitment of limited advisory capability	Relatively easy – recruitment of modest advisory capability	Difficult - owing to the current lack of a reliable baseline and more detailed business case	Very Difficult - owing to the current lack of a reliable baseline and more detailed business case	Moderate – requires significant analysis of current landscape and supporting data

Based upon the analysis above, Option 6 would be preferred.

3.6 Economic Appraisal

The Economic Appraisal would normally provide financial projections for each of the 6 options above, in terms of their expected costs and associated benefits. It would show the expected costs and benefits by year over the project's lifecycle, with each year's figures discounted to produce a "Net Present Cost" or "Net Present Value" for each option.

At this stage of the Digital Forensics Project, there is insufficient operational and financial data to undertake such an analysis. Consequently, this Strategic Outline Case is currently limited to the options analysis set out in section 3.5.

If selected, the preferred option from that analysis will involve the production of a comprehensive Outline Business Case for Digital Forensics, which will include a full economic appraisal of a range of options for supporting digital forensics into the future.

3.7 The Preferred Option

Based upon the analysis of the current short-list of 6 options set out in section 3.5, the preferred option is Option 6. The scope of Option 6 is to:

- Establish an in-house / police-led advisory capability covering all techniques and capabilities involving the acquisition, preservation, analysis and presentation of digital data for evidential use in the criminal justice system, which will work closely with the DII and Digital First programme to ensure cohesion of service operating models and
- Undertake the research and engagement needed to produce a comprehensive Outline Business Case to determine whether it would be beneficial to rationalise, aggregate or integrate into a national Forensic Capability Network any of the digital forensic capabilities that are currently delivered by individual police forces or groupings.

The scope of the services to be delivered in support of Option 6 are set out in section 4.2 (Commercial Case).

3.8 Estimated Costs

The table below provides an estimate of the cost of supporting Option 6 during the period from April 2018 to March 2020 i.e. the period covered by the Police Transformation Fund. Please note that these figures will be refined during the Outline Business Case stage and may change if the associated economic appraisal suggests a different resourcing mix.

Table 8 – Estimated Cost Profile for Option 6

Cost Heading	2018/19 £'000	2019/20 £'000	Total £'000
Digital Forensics Advisory Team	594	1,456	2,050
Business & Technical Leadership, Analysis, Design & MI / BI	235	616	851
Business Case, Funding Model & Procurement / Sourcing	167	240	407
Project Management, Business Change, Training & Communications	254	438	692
Totals	**1,250**	**2,750**	**4,000**

4. The Commercial Case

4.1 Introduction

This section of the Strategic Outline Case outlines the recommended approach to the provision of goods and services in relation to the preferred way forward, as described in the Economic Case.

4.2 Required Services

At this stage of the Digital Forensics Project, the proposal only involves the creation of a "Digital Forensics Advisory Team", which will be able to work with the NPCC Digital Forensics Board and the DII Programme to:

- establish a national authority for Digital Forensics with leadership over technical requirements, quality and processes;
- construct a detailed baseline of force digital forensic capabilities and initiatives, including contracts, procurement and change projects, and make equivalent assessments of demand;
- forge effective public / private / academia partnership to undertake research into future capabilities (emerging and potential) to inform future focus and investment;
- cover the appropriate breadth and depth of digital forensics expertise to support forces in meeting their 'digital forensic' challenges;
- create, along with the DII Programme, a service operating model for a broad range of investigative / forensics scenarios, providing clarity on capabilities and techniques and how best to deploy them;
- work with forces to address current shortfalls in digital forensic support skills, notably the availability of technicians to support frontline digital forensic services;
- create effective links with OEMs to gain access to appropriate data and technical support;
- work with forces and other stakeholders to create a catalogue of approved / endorsed capabilities and techniques;
- work with forces, the Forensic Science Marketplace Group and potentially the Police ICT Company to help procure new capabilities / rationalise existing capabilities;
- support forces with short-term ISO17025 and medium-term ISO17020 accreditation activities (aligned to the related Standards and Accreditation Project);
- define and construct the Digital Forensics elements of the TF learning and development programme;
- represent forces and work with the FSR to produce quality standards, operating models and codes of conduct, which can keep pace with digital forensics;
- produce recommendations, supported by a business case, for the creation of a resilient and future-proofed network of digital forensic capabilities, forming part of an integrated forensics capability and incorporating networking arrangements for evidence management and sharing of intelligence, aligned to the agreed service operating model;

- design a new funding model to support a sustainable, consistent, integrated, quality assured network of digital forensic capabilities.

4.3 Potential for Risk Transfer

The preferred way forward involves creating a "Digital Advisory Team" from a combination of in-house police resources and external support provided, on a flexible delivery resource basis, through the existing Transforming Forensics Programme Delivery Partner contract, which was competed using the Digital Outcomes and Services (DOS2) Framework in July 2017 and is held by Dorset Police.

There is scope within this contract for specific deliverables to be commissioned on a fixed price basis, and this option will be exercised if it is likely to offer best value. This would effectively transfer risk for producing those specific deliverables to the Delivery Partner.

4.4 Proposed Charging Mechanisms

At this stage of the Digital Forensics Project, the proposal is to fund the newly created "Digital Forensics Advisory Team" exclusively from Police Transformation Fund (PTF) grant.

Any continuation of the capability beyond the PTF grant period (31 March 2020) will be subject to acceptance of a separate business case, which will include the associated proposed charging mechanisms. The need for such a capability will be evaluated as part of the recommendations and business case to be produced by this project (see 4.2), for the creation of, and ongoing support to, a resilient and future-proofed network of digital forensic capabilities. It will also reflect the proposed charging mechanisms for the ongoing management of the Forensics Capability Network, which is covered in detail within the Transforming Forensics Programme Business Case.

4.5 Proposed Contract Lengths

All contracts for the components of the proposed "Digital Forensics Advisory Team" will be limited to 31 March 2020, in line with the Transforming Forensics Delivery Partner contract. Where it makes sense to have shorter sub-contracts, this option will be exercised by the Delivery Partner after consultation with the Contracting Authority.

4.6 Personnel Implications (Including TUPE)

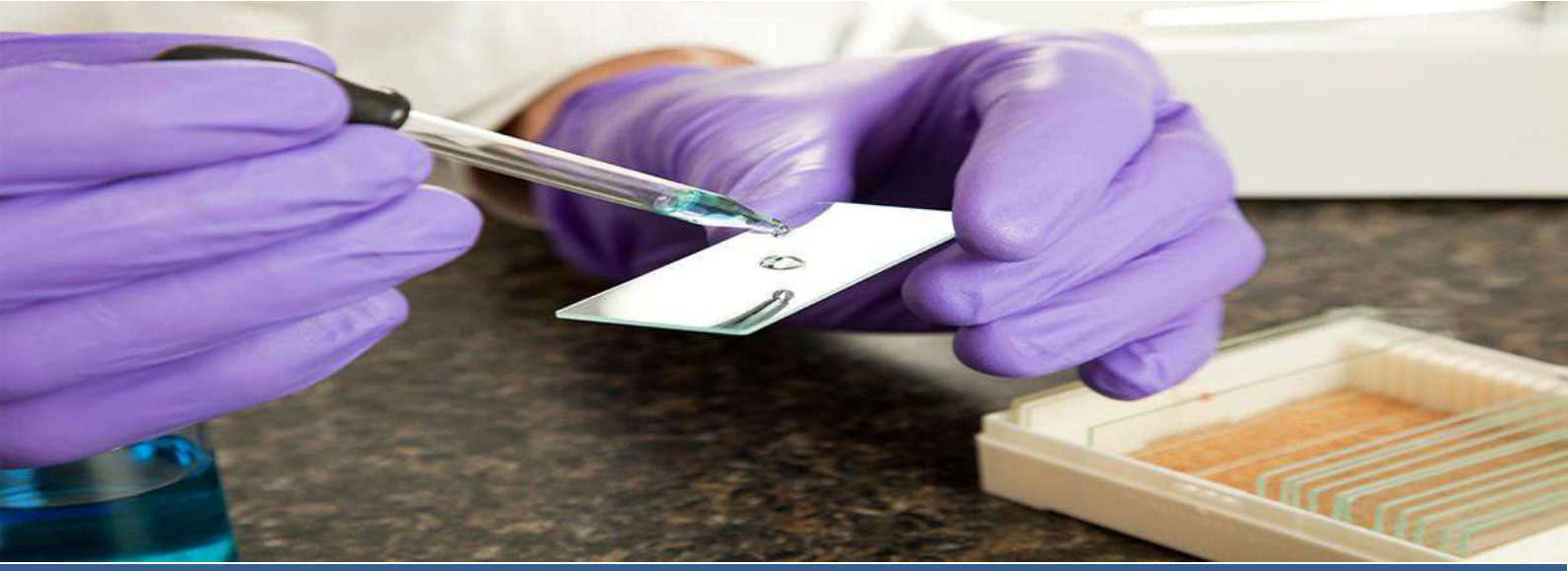
It is not expected that the TUPE – Transfer of Undertakings (Protection of Employment) Regulations 1981 – will apply to this investment since the proposed "Digital Forensics Advisory Team" will be of limited duration and will be staffed through secondments from police forces and short-term contracts. Any longer-term arrangements, which might involve TUPE, will be subject to a separate business case and will reflect the proposals for the creation of a Forensic Capability Network, as set out in the Transforming Forensics Programme Business Case.

4.7 Procurement Strategy and Implementation Timescales

The supporting Delivery Partner contract has already been procured. For this stage of the project therefore, there is no requirement for a separate procurement strategy. Implementation timescales are in line with the proposed project plan illustrated in the Management Case.

4.8 Financial Reporting Standard (FRS) 102 Accounting Treatment

It is not envisaged that the "assets" created by this stage of the Digital Forensics Project, which will largely be documentation and hands-on support, will have any capital value that would need to be reflected in the balance sheet of the Contracting Authority. If this proves not to be the case, any development costs will be capitalised in line with accepted accounting guidelines and be reflected in the balance sheet of the Contracting Authority.



5. The Financial Case

5.1 Introduction

This section of the Strategic Outline Case outlines very briefly the financial implications of the preferred way forward. At this stage of the Digital Forensics Project, the proposal only involves the creation of a "Digital Forensics Advisory Team", to be funded exclusively by Police Transformation Fund grant. As set out in the sections below, the associated financial implications are therefore limited. At a later stage of the project, when recommendations are made for the creation of, and ongoing support to, a resilient and future-proofed network of digital forensic capabilities, the financial implications will be much more extensive. These, however, will be reflected in the Outline Business Case, scheduled to be produced towards the end of 2018.

5.2 Impact upon the Organisations' Income and Expenditure Accounts

The current stage of the project will have no net impact upon the income and expenditure accounts of either the Contracting Authority or participating police forces. The impact will simply be £4 million grant income and £4 million related revenue expenditure, as profiled in the table below.

Table 9 – Estimated Grant and Expenditure

Heading	2018-19 £'000	2019-20 £'000	Total £'000
Police Transformation Fund Grant	1,250	2,750	4,000
Forecast Expenditure	1,250	2,750	4,000
Net Expenditure	**0**	**0**	**0**

5.3 Impact upon the Organisations' Balance Sheets

It is not envisaged that the "assets" created by this stage of the Digital Forensics Project, which will largely be documentation and hands-on support, will have any capital value that would need to be reflected in the balance sheets of either the Contracting Authority or participating police forces.

5.4 VAT (Value Added Tax) Treatment

For the purposes of this business case, it has been assumed that VAT will be fully recoverable. This is because both police forces and Police and Crime Commissioners can recover VAT and have special dispensation under Section 33(2) of the VAT Act, which, subject to a 5% de minimis limit, allows them to recover all their input VAT even where the associated expenditure relates to a VAT-exempt service. The same applies to local authorities.

As a result, VAT has not been added to either the income or expenditure figures shown in this case.

5.5 Overall Affordability

Since the current stage of this project will be funded exclusively from grant and will have no impact upon participating forces' income and expenditure accounts or balance sheets, it is affordable. Overall affordability will be a significant consideration in the Outline Business Case, which is scheduled to be produced by the end of 2018, but is expected to be extremely positive, given the significant affordability challenges currently faced by police forces with the existing operating model (see section 2.5).

6. The Management Case

6.1 Introduction

This section of the Strategic Outline Case outlines the project management arrangements proposed for the creation of the "Digital Forensics Advisory Team", together with an illustrative project plan.

6.2 Programme Management Arrangements

The management arrangements in place for the overarching Transforming Forensics Programme are set out in detail in the Transforming Forensics Programme Business Case and are therefore not replicated in detail here. In summary, though the TF programme is being delivered through the NPCC Forensic Portfolio and will be governed by a newly established Executive Programme Board (EPB). It will link into other national programmes as follows to ensure cohesion across the broader policing landscape.

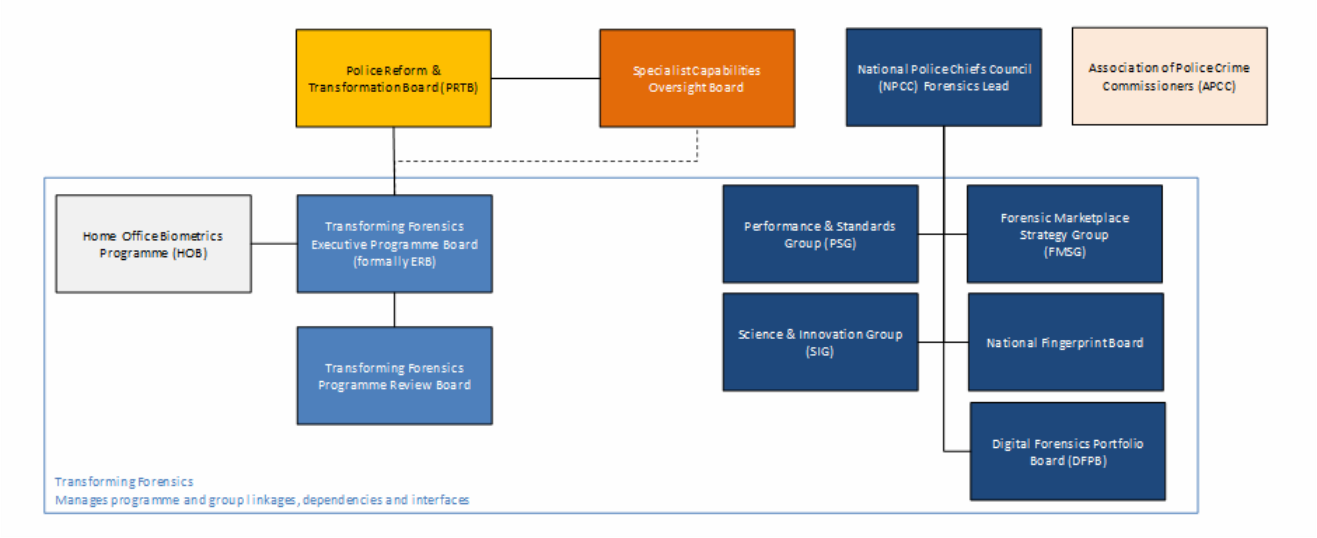


Figure 3 Programme Governance Board Relationships

The proposed governance framework follows best practice from MSP and is compliant with the principles of PRINCE2.

Detailed programme management will be organised as follows.

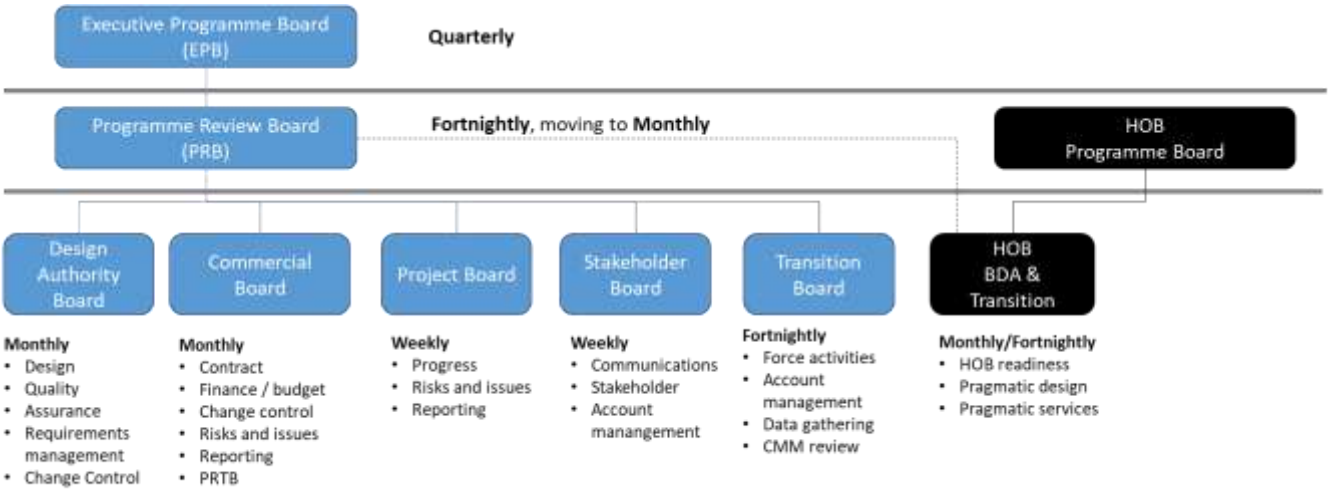


Figure 4 – Transforming Forensics Programme Governance Structure

6.3 Project Management Arrangements

6.3.1 Project Reporting Structure

The project reporting structure for the Digital Forensics Project, as part of the broader TF Programme, is illustrated below.

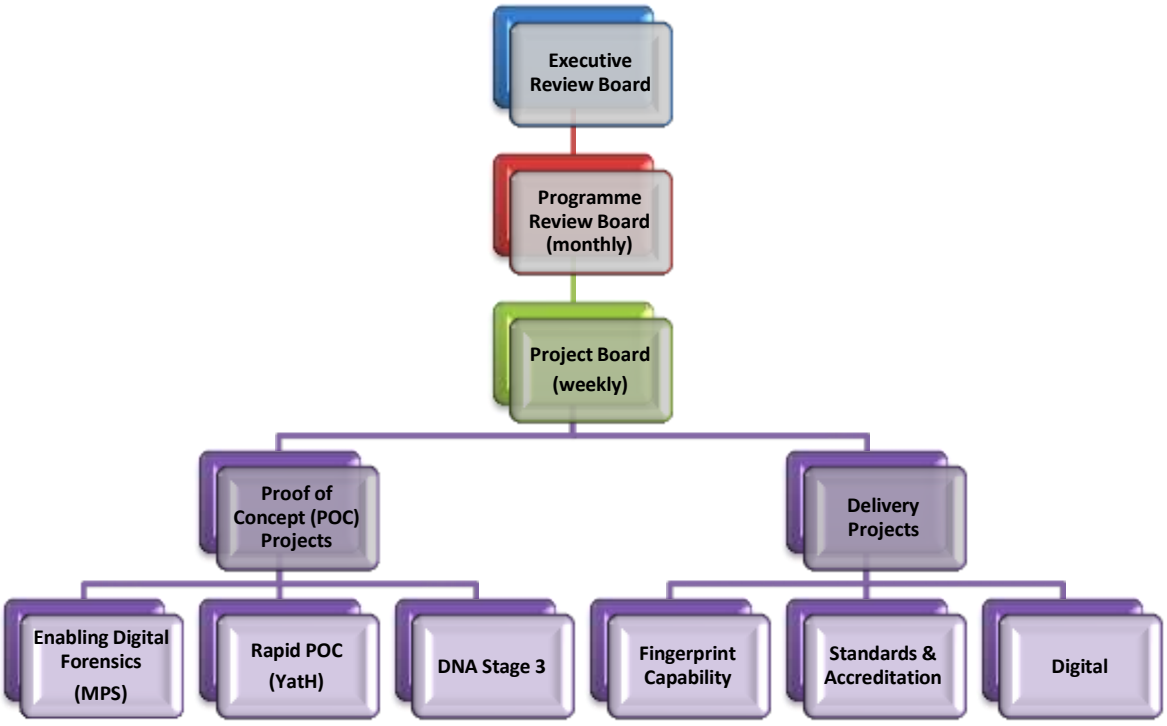


Figure 5 – Transforming Forensics Project and Programme Reporting Structure

6.3.2 Project Roles and Responsibilities

The roles envisaged for the Digital Forensics project and their associated responsibilities are set out in the table below.

Table 10 – Project Roles and Responsibilities

Role	Responsibilities
Business Lead	To lead the project from a policing perspective, ensuring that the project is focused upon the areas that will bring most benefit to policing and public safety; is closely aligned to the DII and Digital First Programmes; is effectively represented at senior levels; and becomes the catalyst for the creation of a national authority for digital forensics. Will also be responsible for devising a new service operating model, in conjunction with the Technical Lead and the DII Programme, and for supporting the "Standards and Accreditation" project in working with the FSR to produce quality standards, operating models and codes of conduct, which can keep pace with digital forensics
Technical Lead	To lead the technical aspects of the project and have lead responsibility for the creation of the detailed baseline, Technology Readiness Level roadmap, and catalogue of endorsed capabilities and techniques. Will also be responsible for forging effective links with OEMs; for devising a new service operating model, in conjunction with the Business Lead and the DII Programme; and for supporting the Business Lead and "Standards and Accreditation" project in working with the FSR to produce quality standards, operating models and codes of conduct, which can keep pace with digital forensics
Digital Forensics Advisory Resources	To provide support and subject expertise to both the Business and Technical Leads; to provide appropriate breadth and depth of digital forensics expertise to be able to support police forces in meeting their digital forensics challenges; and to provide appropriate input for the creation of a Learning and Development programme for digital forensics
ISO Accreditation Support	Aligned to the TF "Standards and Accreditation" project and able to provide the appropriate digital forensic science input to the "Standards and Accreditation" project, as well as supporting forces in meeting their day-to-day challenges
Business Case Lead	To lead on the production of Outline and Full Business Cases, as appropriate; for the creation of a resilient and future-proofed network of digital forensic capabilities, forming part of an integrated forensics capability and incorporating networking arrangements for evidence management and sharing of intelligence, aligned to the agreed service operating model. Also responsible for devising an appropriate funding model to support the above

Role	Responsibilities
Procurement and Sourcing Support	To lead on all associated market engagement and procurement / sourcing activities
Programme, Project Management and Communications Support	Aligned to the overall TF Programme and responsible for providing programme, project management and communications support to the Digital Forensics Project. This will also incorporate a dedicated Project Manager role.

6.3.3 Project Plan

The illustrative plan for the current stage of the Digital Forensics Project is depicted below.

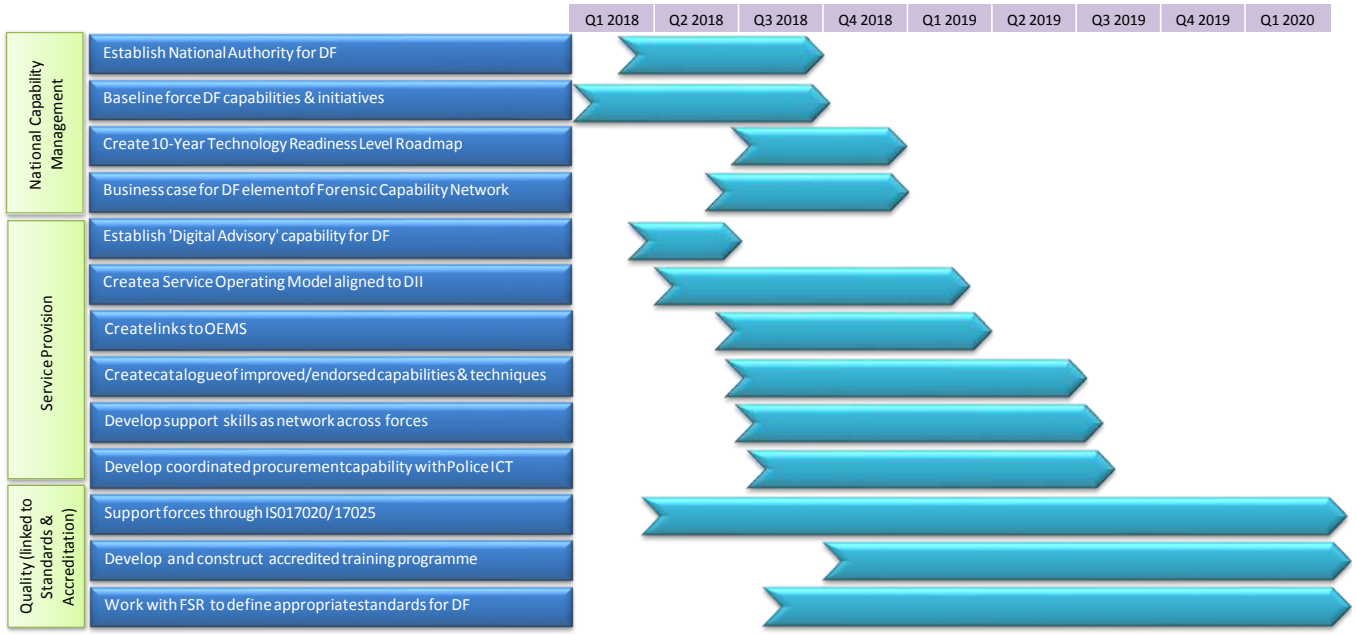


Figure 6 – Illustrative Project Plan

6.4 Outline Arrangements for Change and Contract Management

Contracts for the components of the "Digital Forensics Advisory Team" will be held by either the Contracting Authority (Dorset Police) or the Delivery Partner (KBR), as agreed between the two parties and reflecting the nature of the delivery resource i.e. police force secondment or external resource. These arrangements will be overseen by the TF Programme's Commercial Board, as illustrated in section 6.2.

6.5 Outline Arrangements for Risk Management

The TF Programme has adopted a very rigorous and professional approach to RAID (Risk, Assumption, Issue and Dependency) management, with the Programme Review Board keeping them under constant review. The most significant risks facing the Digital Forensics Project are set out within the Strategic Case (section 2.9).

6.6 Outline Arrangements for Benefits Realisation

The overall approach for the TF Programme and its constituent projects is benefits-focused. A Benefits Management Strategy has been prepared and a robust benefits realisation plan is being developed and will be monitored throughout the programme's lifecycle.

So far, the Programme has developed:

- a detailed analytical model that is designed to work at a small enough scale (i.e. by project by force by service-line by expenditure type by month) that it can be used longer term by the TF Programme and beyond for benefits tracking (e.g. comparing estimated benefits with actuals);
- a Management Information pack that will start to collect activity data, which, when combined with financial information, will enable the Programme and its constituent projects to calculate unit costs (the key to efficiency measures);
- a Capability Maturity Model, which provides a baseline and measure for non-financial progress;
- benefits maps for each project, linking from the project outputs to the Policing Vision 2025.

The TF Programme will be supported by dedicated "business readiness and change managers", who will be responsible for monitoring the early benefits as they are delivered by both the programme and participating forces. As the programme develops, the benefits will be handed over to operational owners with responsibility for realising the benefits in their areas.

6.7 Outline Arrangements for Post Project Evaluation

The outline arrangements for the project evaluation review (PER) and post implementation review (PIR) are set out below and are in accordance with project management best practice.

6.7.1 Post Implementation Review (PIR)

The PIR will appraise how well the project was managed and whether it delivered to expectations. This will be undertaken by an Independent Evaluation Team, which will be appointed with support from the Home Office Crime Analysis Unit and Government Trials Advisory Panel. An Independent Evaluation Team, appointed with the same support, is already in place and has been assessing the impacts and benefits of the digital & rapid forensics "proof of concept" projects (fingerprints, DNA and digital forensics kiosks) currently being delivered under the TF Programme.

6.7.2 Post Evaluation Reviews (PERs)

The PER ascertains whether the anticipated benefits have been delivered. As with the PIR, this will be undertaken by an Independent Evaluation Team, which will be appointed with support from the Home Office Crime Analysis Unit and Government Trials Advisory Panel.

6.8 Gateway Review Arrangements

The TF programme has already undertaken one independent review, based on an (Office for Government Commerce) OGC Gateway Review 0 Strategic Assessment (November 2017). The aim of this review was to provide very early feedback to TF on the progress being made and identify any areas that would benefit from greater focus. Further gateway reviews will be undertaken throughout the programme's lifecycle and will be aligned to bother project and programme milestones and deliverables.

6.9 Contingency Plans

Progression of the Digital Forensics project, as outlined in this Strategic Outline Case, is reliant upon the grant of £4 million from the Police Transformation Fund. If a lesser amount is awarded, the scale and scope of the project will be reduced in accordance with participants' wishes and the direction of the Executive Programme Board.