

Meeting	Authority Meeting
Date	24 March 2021
Location	Video Conference
Title of Paper	Implementation of Cyber Strategy
Presented By	DCC Malcolm Graham, Crime and Operational Support
Recommendation to Members	For Discussion
Appendix Attached	Yes Appendix A – Cyber Strategy Implementation Plan FY 21/22

PURPOSE

This paper provides an update to the Board in relation to the Police Scotland Cyber Strategy and presents the associated Implementation Plan for financial year 21/22, further to discussions at the Board meeting on 30 September 2020.

Members are invited to discuss the contents of this paper.

1. BACKGROUND

- 1.1 The Police Scotland Cyber Strategy was approved by the SPA Board when it was presented by DCC Graham on 30 September 2020 and an update was provided in relation to the developing Implementation Plan to the Police Scotland Strategic Leadership Board (SLB) and SPA Members Seminar in February 2021.

The Cyber Strategy Implementation Plan (FY21/22) (Appendix A) was presented to the SLB on 10 March 2021, where it received approval. It is now submitted to the SPA Board for discussion.

2. FURTHER DETAIL ON THE REPORT TOPIC

- 2.1 The plan sets out the increasing and complex demand presented by Cyber enabled and dependent crime and recognises that delivery of the Strategy is wide-ranging and cross-cutting within Police Scotland, so a substantial amount of co-production and development will be required, e.g. in relation to protecting young people, reducing online harm and Local Policing design.

Creation and implementation of the Strategy is within the context of a global growth of cybercrime and, more locally, a significant increase in victims within Scotland during the ongoing pandemic.

Whilst Police Scotland has well established relationships with public, private and other sector partners tackling such issues within Scotland and wider UK, we need to develop these to enhance our joint understanding and intervention capabilities to reduce threat and harm.

The rapidly developing nature of cyber dependent and enabled crime, including through the use of novel technologies, means that we must act now to ensure that our support to victims and potential victims and our impact on criminal enterprises can be maximised.

It is recognised that delivery of the Strategy will require an agile and responsive approach to developing trends and threats within the digital arena, therefore the Implementation Plan may be subject of review and re-planning to ensure that associated work serves to address the greatest threats to Scotland, its citizens and our organisation.

Our approach will continually seek to balance Rights with our public duty to maintain and enhance safety and security. Consequently, our desire to generate an open discussion with the public around this topic will recognise our obligations and outline the challenges

that we face in tackling such criminality, including in relation to our use of existing and developing technologies.

Underpinning all of our activities in relation to the plan will be our ambition to support both our 'Joint Strategy for Policing' and the recently published Scottish Government Strategy, 'A changing nation: how Scotland will thrive in a digital world', to produce positive outcomes for our communities and businesses. Implementation will include supporting effective internal financial planning and will be closely aligned to the developing Strategic Workforce Plan, our Modernised Contact and Engagement Programme and other key transformational activities.

The Design Phase of the Plan is currently ongoing and will define future processes, structures, technologies and finance requirements.

Relevant governance arrangements are being refreshed, with oversight being provided by DCC Graham as Chair of the Cyber Strategy & Capabilities Change Co-ordination Board and ACC Campbell and DCIO Andrew Hendry as SRO's in relation to related Programmes.

3. FINANCIAL IMPLICATIONS

- 3.1 Projected costs are outlined within the Plan. In summary, £4,106,249 is currently budgeted within FY 21/22, including in relation to the Police Scotland Cyber Security Strategy. Costs associated with the Cyber Security Strategy of £1,183,592 are also projected for FY 22/23. Other costs are currently being defined and will be reported through relevant Business Cases.

4. PERSONNEL IMPLICATIONS

- 4.1 Implementation of the Plan will involve a re-modelling of Police Scotland resources in order to build capability and capacity to deal more effectively with Cyber enabled and dependent crime and to work in partnership to further embed a prevention and harm reduction approach. This will involve re-prioritising existing budgeted posts and consideration of our specialist policing structures and Local Policing arrangements.

Initial requirements to meet existing Digital Forensics and Cyber Investigation demands have previously been outlined in the Strategic Workforce Plan submission and work will continue in that regard as the Implementation Programme progresses.

As the Programme develops, engagement will be undertaken with Staff Associations and Unions, as well as directly with affected staff. Details regarding personnel implications will be provided further in related Business Cases, JNCC submissions, governance reporting and in relevant reports and updates to SPA members and Boards.

5. LEGAL IMPLICATIONS

5.1 There are no specific legal implications at this time.

6. REPUTATIONAL IMPLICATIONS

6.1 There are no immediate reputational issues associated with the paper.

Longer-term, potential reputational issues will relate to the manner in which Police Scotland progress implementation of a technology related Programme. Such issues will be mitigated through appropriate governance and oversight, public consultation, external scrutiny and challenge, coupled with effective internal and external communications.

7. SOCIAL IMPLICATIONS

There are no immediate social implications at this time.

8. COMMUNITY IMPACT

8.1 Our approach to engagement and communication with the public, communities, partners and key stakeholders is a critical area of the work to implement the Cyber Strategy, recognising both the public interest and potential impacts of both Cybercrime and our potential future use of emerging technologies and investigative methods.

It is recognised that implementation will require an open, transparent and ongoing conversation in Scotland to ensure our consideration of new policing is done with the consent of the public, to ensure the continued legitimacy of policing.

A high level approach to public engagement is being developed by the Programme team, supported by our Strategy and Innovation Department. The objectives of the engagement approach are:

OFFICIAL

- To be open, transparent and lead a wide reaching conversation on the development of new approaches to operational policing in a digital age.
- To continue to build trust and public confidence in policing, ensuring all appropriate parties are involved in new policing approaches to retain legitimacy and consent.
- To communicate effectively and address any public concerns openly as we implement our Cyber Strategy and the new approaches this will bring for the policing service in Scotland.
- To engage and collaborate with partners and key internal and external stakeholders, ensuring a cohesive evidence base to support decision making with the Scottish Police Authority and to offer assurance to Scottish Government and Parliamentary Committees.

Public engagement activity will be initially undertaken to align with Police Scotland's overarching engagement framework and the developing Cyber Implementation Plan to enable the right conversations on the key questions at an early stage.

In addition, a range of partner and stakeholder engagements will be in place as the plan is implemented. This will include agreement of approaches with the Scottish Police Authority and, subject to the wider proposals for Police Scotland oversight and governance, setting up a Professional Reference Group with expertise from all sectors and academic contributions. The group will share best practice, leading research findings and provide both challenging and enabling collaboration as new approaches to policing are developed.

We will maintain and build our commitment to the recently formed Independent Advisory Group on the Police Use of Technology, chaired by Dr Liz Aston (Scottish Institute for Policing Research) and use this to build our understanding of public, academic and expert views and opinions on the proportionate and effective use of data and technology to protect the people and businesses of Scotland.

Our engagement with the public in a way that informs our approach to delivering the Cyber Strategy is critical. We will seek to inform them of the challenges that we face in this arena and to work with them to test how we could most effectively and ethically achieve our policing purposes of maintaining safety and wellbeing and tackling offenders, whilst prioritising fundamental Rights. We will seek to generate public debate and discussion and to make decisions

around implementing practices and technologies which achieve the support of the public in order that we can achieve our objectives together.

9. EQUALITIES IMPLICATIONS

9.1 It is recognised that implementation of the Strategy will require detailed consideration of Equalities matters, both in terms of what is delivered and how. Our obligations under the Equalities Act 2010 will be respected at all times, including when procuring services. An Equalities and Human Rights Impact Assessment and Data Protection Impact Assessment will be conducted in due course.

10. ENVIRONMENT IMPLICATIONS

10.1 There are no immediate environmental impacts associated with the paper, but given that the Implementation Programme will involve the use of technologies, this element will be developed as work progresses.

RECOMMENDATIONS

Members are invited to discuss this contents of this paper.

Police Scotland Cyber Strategy Implementation Plan 2021/22







KEEPING PEOPLE SAFE IN THE DIGITAL WORLD



POLICE
SCOTLAND
FOR THE PEOPLE

SCOTTISH POLICE
AUTHORITY

Contents

Introduction	3
Objectives and enablers	8
 Enablers	12
 Locations and Assets	19
 Demand Analysis	19
 Information	211
 Organisation	244
 Management	28

Introduction

The Police Scotland Cyber Strategy 'Keeping People Safe in the Digital World' was approved by the SPA Board on 30 September 2020.

The ambition of this strategy is to bring about the comprehensive change necessary to become a centre of excellence in digital and cyber policing. By exploring the different elements of our organisation, we have developed our objectives and designed enablers to direct our transformation.

This is an enabler strategy, underpinning and supporting the Joint Strategy for Policing (2020), Policing for a Safe, Protected and Resilient Scotland. The strategy sets out Police Scotland's approach to contribute effectively to the following strategic outcome and objective:

Strategic outcome 1: Threats to public safety and wellbeing are resolved by a proactive and responsive police service

Objective 1: Keeping People safe in the physical and digital world

In Policing for a safe, protected and resilient Scotland, we committed to the development of a pioneering Cyber Strategy for Police Scotland with the aim of enabling us to transform our capacity and capability to respond to threats and establish various ways to prevent, disrupt and respond to the ever more inventive and complex use of digital tools and new tactics, often originating from beyond our borders.

Cyber enabled and cyber dependent crime has been increasing for a considerable period of time and this has escalated further during the COVID-19 pandemic. This is an area of increasing risk and Police Scotland must ensure that our policing model can respond effectively.

The global aspects of Cybercrime, rapid development of criminal techniques and complexity of both the partnerships and technologies required to address it, means that achieving our ambitions will require substantial time, investment and development. Whilst we aim to maintain pace with criminal enterprises, we must build capacity and capabilities within our own organisation to ensure that delivery of the Strategy is both sustainable and impactful. Our aim is to build on existing structures, processes and strengths, but to achieve our overall objectives we will look to create additional functionality, skills and structures, the challenges of which will require us to do so in an incremental manner.

Nationally, good progress has been made to date, including the roll out of digital triage and mobile devices and addressing legacy issues to streamline our core

operational systems through the Digitally Enabled Policing Programme. We are also well-placed as a key partner within the wider ecosystem of global law enforcement and other agencies developing and delivering approaches to interrupt threats from Cybercrime, meaning that we can both influence and learn from wider experiences and developments.

The Cyber strategy has been designed and developed with the support of a strategic oversight group Chaired by DCC Graham. A full range of strategic assessment, research and a landscape review was undertaken along with an extensive range of internal and external stakeholder engagement. The views of the public and communities were sought as part of the consultation on the strategy and have been considered as the cyber strategy has been developed.

Case for change

The case for change is driven by a complex set of challenges that modern policing in Scotland is facing, namely:

- Escalating risk of threat and harm
- Changing demands
- Enabling effective policing

Escalating risk and harm

In recent years there has been a steady trend of cyber enabled and cyber dependant crime increasing in Scotland, and the wider UK. As communities increasingly spend more of their time using internet-connected devices and residing in online spaces, exposure to criminal and malicious actors has increased in tandem. Underreporting of cybercrime presents a significant challenge to policing as we know that the data available doesn't clearly represent the true scale of this criminality. In order to effectively safeguard these spaces we must make our presence more visible online, ensuring education and prevention services are available and accessible to the public.

Whilst Police Scotland aims to mitigate risk and minimise the harm caused to individuals and our communities by Cybercrime, the global reach of criminal enterprises often means that those responsible for committing such crime are located far out with our own borders. Not only does this present specific challenges in terms of investigation and enforcement, it means that we must identify and develop the most effective methods of preventing victimisation and reducing harm locally and in partnership, raising public awareness of ways to avoid becoming a victim and building effective methods of supporting people, businesses and organisations to defend against the increasing ingenuity of those who wish to prey on them.

The cyber threat posed to the citizens of Scotland can be considered from two broad perspectives

- The criminal opportunities / threats that exist in a society increasingly dependent upon digital and interconnected technology that we use, carry and wear (predominantly cyber enabled), and;
- The wider threat posed to us via the potential compromise of our businesses and infrastructure (predominantly cyber dependant).

It is evident that the threat to Scottish communities, business and infrastructure from to cybercrime is truly global. The uniquely borderless nature of cybercrime means that we are as vulnerable in this regard to threat actors on the other side of the world as we are to one operating in Scotland. In this context our cyber threat assessments have to consider global trends, developments and criminal capabilities. We in turn use our awareness of these threats and through our widening collaborative reach into partners such as NCSC and SBRC, we ensure that the awareness and mitigation measures that can be deployed are taken wherever possible.

Changing demand

It is clear that the frontline of policing in Scotland is being blurred by the use of technology to aid, and facilitate crime. These criminal acts are steadily increasing in their frequency and complexity, placing new forms of demand on our resources and personnel. To meet these changing demands we must commit to implementing a new policing model that recognises technology as both a challenge and an enabler for modern policing.

Child Protection

Since the creation of Police Scotland in 2013 there has been a 1617% rise in Online CSAE referrals from industry and wider law enforcement. Referrals are assessed, developed and allocated for investigation as a National Online Child Abuse Prevention (NOCAP) investigation. 2019/20 saw a rise of 23% in referrals which resulted in a 49% increase in actionable NOCAP enquiries.

The 2019 HMICS Thematic Inspection of Police Scotland's response to Online CSA resulted in 10 recommendations for the Force in respect of the overall end-to-end process from Online CSAE referral to investigation. A pertinent feature of the HMICS Thematic Inspection was the notion that Police Scotland specifically, was not as effective in its pro-active policing of Online CSAE as it might or should be, including lawful exploitation of covert tactics. This is presently being addressed through the exploitation of new capabilities.

The most prevalent of sexual offences against children have been to cause or coerce to see/hear sexual images/content; communicating indecently; and possession/distribution of indecent images of children (IIOC). Other crime types of lower volumes also continue: coercing/encouraging a child to engage in sexual activity online, disclosure of an intimate image/revenge porn; grooming; discussing child sexual abuse; voyeurism; and sextortion. During January 2021 over 69% of intelligence logs submitted onto Police Scotland intelligence systems related to child sexual abuse.

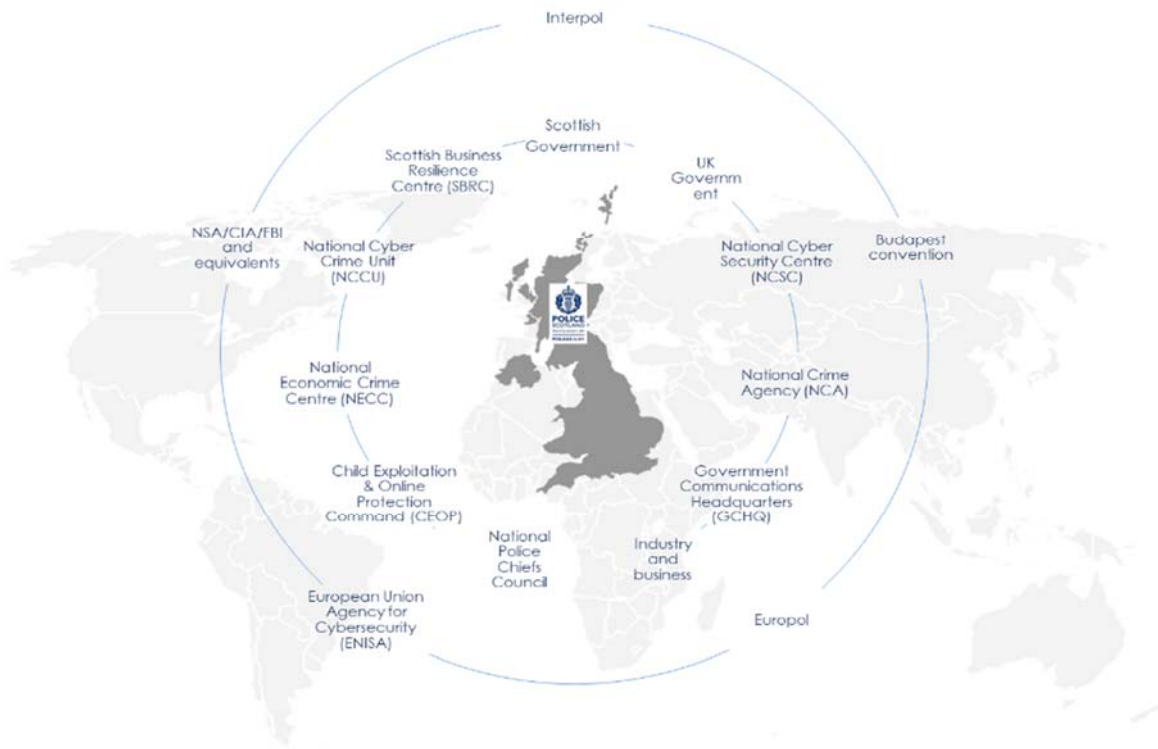
Enabling effective policing

With technology rapidly developing and becoming increasingly accessible to the public, policing and safeguarding in online spaces has never been more important. Undertaking this represents a significant shift in our operational policing model, and will require us to push into uncharted territory for policing in Scotland. In order to navigate this effectively, we must develop clear strategic direction to chart the best way forward, and ensure that we work collaboratively to create approaches supported by our partners and communities.

Implementation of this Strategy will build confidence with the public that Police Scotland are appropriately skilled and equipped to deal effectively with Cyber enabled and dependent crime. Improving methods of engagement with service users will allow us to respond more promptly and effectively to their needs, ensuring that we can both meet changing expectations and deal appropriately with reducing vulnerability and harm.

Recognising the international reach of Cyber enabled and dependent crime, we will enhance and develop our capabilities with national and international law enforcement agencies. Our approach will, however, focus attention on those investigations which can have the greatest impact on protecting the people of Scotland and enabling partner agencies to also reduce harm by taking intervention action.

Our ambition to lead the fight against Cyber enabled and dependent crime relies heavily on our existing and future relationships with UK and global partners. Recognising the multi-faceted and complex nature of Cybercrime and the range of developments required to achieve our strategic ambitions, we seek to create long-term collaborations which will enhance our expertise, provide access to learning and build alliances that can reduce risks and enhance our capabilities. Our established partnerships at the multi-agency law enforcement focussed Scottish Crime Campus act as a platform for our joint objectives and provides a central focus for Cybercrime investigations in Scotland.



Rights and Ethics / SPA Engagement

A 'Rights' based approach will underpin implementation of our Cyber Strategy, with an ethical approach enshrined in our use of data and new, emergent technologies and approaches to dealing with Cybercrime.

Recognising public concerns regarding the police use of data and technology, alongside the highly politicised nature of modern policing, our approach will seek to include generating early, open dialogue with the public, including interest groups and the academic sector. We will seek to pro-actively consult and engage with the public and interested parties early in the course of our considerations regarding the use of data and technology and work with them to gain a shared understanding of the potential benefits and challenges.

We will ensure a strong and consistent ethical oversight that is open to scrutiny and maintains public confidence.

Our approach to policing is built on our shared values of fairness, integrity, respect and supporting and enabling human rights. As we live more of our lives online and we see risk and vulnerability increase, we will seek to strike the right balance between privacy and protection.

As one of the largest organisations in the Scottish public sector we have a responsibility to protect the service we provide from both cyber-attack and systemic vulnerabilities. Policing in Scotland is based on consent and trust, and we must safeguard our own cyber security and resilience in order to exercise our duties to the public.

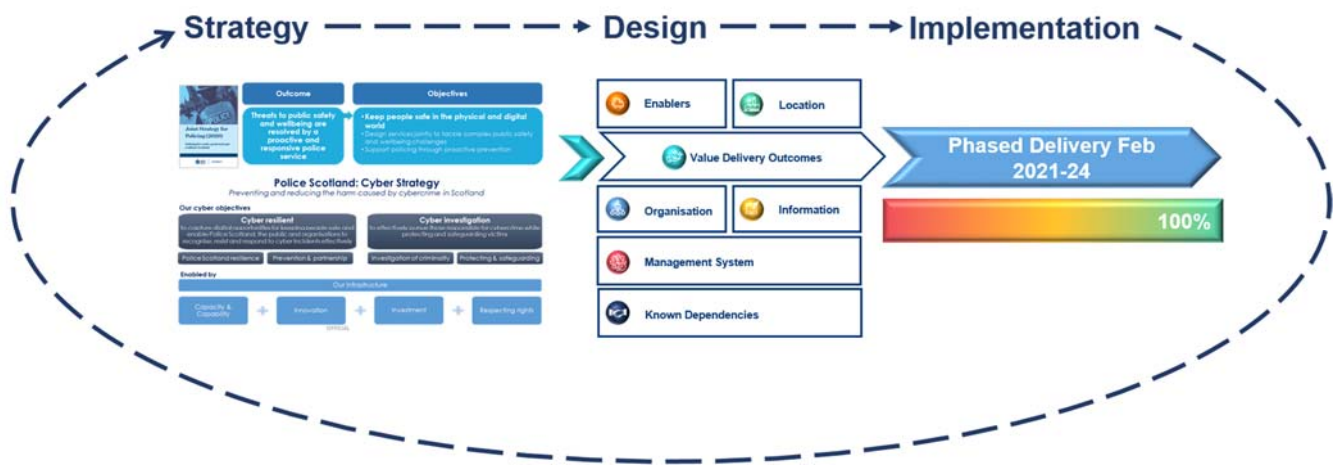
Objectives and enablers

The strategy focuses on five objectives to address a range of key internal and external areas where the service needs to design, develop and implement new approaches for the future.

Police Scotland Resilience	Ensuring that Police Scotland is resilient and able to respond to shifting threats
Prevention	Working holistically and sustainably to prevent cybercrime by developing a public health approach
Partnership	Our partnership will be developed, strengthened and expanded to ensure that our collective efforts can maximise positive outcomes
Investigation of Criminality	Making Scotland a challenging place for cyber criminals to operate by increasing our visibility in the physical and virtual world
Protecting and Safeguarding	Ensuring that our focus on protecting and safeguarding those at most risk of harm continues to be at the forefront of all we do

Recognising the pace of challenges associated with Cybercrime and the impact that it has on our communities, the Cyber Strategy and its implementation will be cyclical, with Design, Implementation and the changing nature of Cybercrime continually informing the Strategy itself over coming years.

Strategy Design and Implementation Cycle



Whilst we will move rapidly to delivering improvements to our capability, capacity and infrastructure it is recognised that delivery of our Strategy will take place over several years, during which time we will fully align delivery to our Strategic Workforce Planning, ensuring that our commitment to tackling Cybercrime is in accordance with our wider organisational plans and priorities and demand, in order to ensure that we meet the changing needs of the public. A change in workforce profile will be required to meet such changing demands, with a need to increase and re-model our staffing approach to prevention and investigations.

We will adopt a phased approach to implementation and investment, ensuring that our prioritisation focusses on building capacity to deal with existing and future threats and risks. Whilst much of the work will be driven by the Implementation Team, delivery of the Strategy is wide-ranging and cross-cutting within Police Scotland, so a substantial amount of co-production and development will be required, for example in relation to protecting young people or reducing online harm.

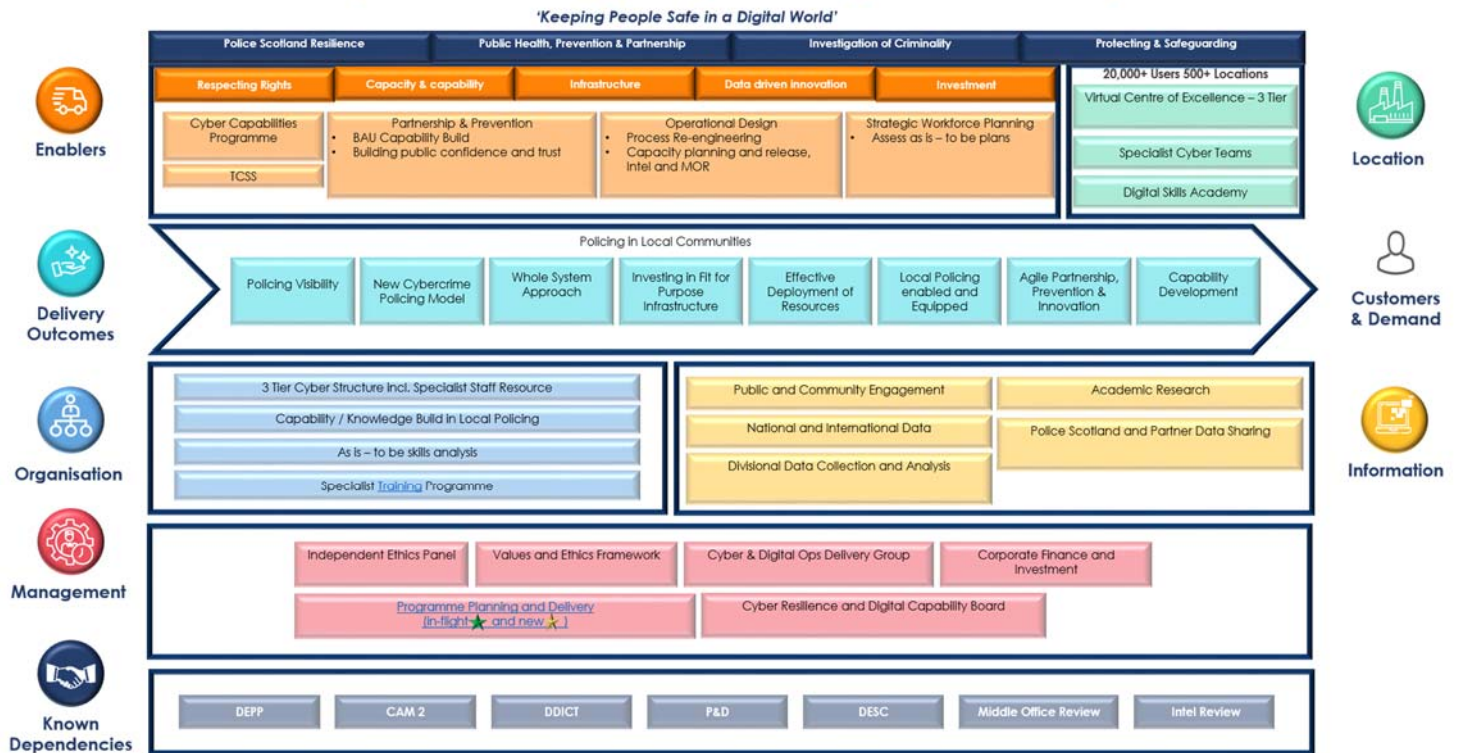
<p>Phase 1 Planning and Early delivery</p>	<p>Design – we will define key projects and deliverables, financial requirements and timelines.</p> <p>Re-alignment of resources – we will strengthen our Digital Forensics and Cyber Investigation capabilities by re-modelling our resources in accordance with our Strategic Workforce Plan.</p> <p>Strategic Projects – we will establish key Strategic Projects and related governance, supported by appropriate SME's and Change resources. Business Cases will be developed for initial projects. This will include our commitment to ISO accreditation for Digital Forensics and improvement of managers data for Cyberkiosks.</p> <p>Funding – we will define our future funding requirements in line with key objectives and priorities.</p> <p>Partnership and Prevention – we will continue to develop our harm reduction activities in conjunction with the private, public and voluntary sectors to reduce victimisation and identify opportunities to strengthen approaches across sectors.</p> <p>Centre of Excellence – we will develop our approach to creating a Centre of Excellence, in conjunction with partners, to establish Police Scotland as a leader in preventing and responding to Cybercrime.</p> <p>Consultation and Engagement – We aim to be public sector leaders in consulting and engaging with individuals, groups and communities to develop our approach around existing and developing technologies. Placing Rights and Ethics at the heart of our approach, we will test our thinking in the public space, seeking views and feedback, and working with the public, elected representatives and subject matter experts to develop means to tackle Cybercrime which achieve an appropriate balance between privacy and protection. We will create a Professional Reference Group through which we will engage the views of external specialist stakeholders and value their challenge and scrutiny.</p> <p>Public Contact We will develop improved methods for the public to contact us to both seek advice and to report Cybercrime and ensure that our staff have the skills and knowledge to respond effectively.</p> <p>Demand analysis – we will develop our understanding of the impact of Cybercrime on policing, the public and businesses through a greater understanding of available data.</p> <p>Skills and Learning – we will complete a Training Needs analysis, identify methods of addressing skill gaps and increasing awareness amongst our workforce of Cyber related issues and how to deal with them effectively.</p>	<p>Short-term (12 months) (funding dependent)</p>
--	---	---

OFFICIAL

<p>Phase 2 Roll-out and Strategic Projects</p>	<p>Workforce re-design – based on developed demand data, resources will be aligned within Local Policing and Specialist areas to meet Cyber related demand and ensure that our preventative and investigative capabilities are enhanced. The ability of Local Policing resources to deal with Cybercrime and support victims will be strengthened through skills improvement and capacity building. We will also create pathways for staff development and create opportunities for an increasingly diverse set of qualifications, experience and capability to ensure that Police Scotland has the ability to understand and respond effectively to emerging trends.</p> <p>Strategic Projects - finalise and conclude delivery of phase 1 plans and feasibility testing of freshly identified strategic opportunities.</p> <p>Partnerships and Prevention – further development and strengthening of strategic partnerships.</p> <p>Funding – as defined within relevant Business Cases.</p>	<p>Medium-term (1 - 3 years) (funding dependent)</p>
<p>Phase 3 Embedding Cyber capabilities across Police Scotland</p>	<p>Capability – a significant number of officer and staff roles will have been created within the organisation and a step change enhancement in our capabilities will have occurred. Our organisation will have the ability to effectively investigate and/or prevent Cybercrime and be Cyber-resilient.</p> <p>Adaptive – we will be adaptive to developing technologies and criminality and develop new methods and Strategic Projects to remain at the forefront of modern policing and able to tackle digital crime effectively.</p> <p>Funding – future funding requirements will be defined and reflected in relevant Business Cases.</p>	<p>Long-term (3-5 years) (funding dependent)</p>

To support implementation of the Strategy during Financial Year 21/22, an 'Operating Model Map' has been developed, strands of which define key enablers, dependencies, objectives and activities.

Cyber Strategy Operating Model Map



We will achieve the objectives of Phase 1 by progressing the following key Workstreams:

Enablers

Cyber Capabilities Programme

To date, the Cyber Capabilities Programme has delivered the introduction of Cyber Champions, building knowledge of staff within Divisions to support initial investigations and local resilience. It has also supported the implementation of Cyberkiosks to improve our initial assessment of devices and better meet the needs of victims and witnesses, in addition to implementing Cyber Markers, system

OFFICIAL

enhancements and raising awareness around the importance of accurately recording Cybercrime to help identify trends and improve our response.

The Programme is currently progressing the delivery of a modern, replacement Case Management System for Digital Forensics and Cyber Investigations and is currently scoping a Cyber Kiosk Management Information system to support demand analysis and reporting.

In the next 12 months, it will continue planning and scoping activities for a strategic project to support our journey towards ISO 17025 accreditation for Digital Forensics. This will include training, process improvement and technologies and will require investment of both capital and revenue (to be defined). Whilst enhancing our ability to provide crucial evidence in support of prosecutions, many of which are related to the most serious of crimes, this accreditation will address SPA recommendations and will achieve parity with the standards that exist across the wider Forensics landscape.

Work will also be undertaken to introduce a 'Cyber App' to Police Scotland mobile devices to allow enhanced decision making and victim support.

Partnerships, Prevention and Wellbeing

Police Scotland now produce monthly and annual Cyber Threat Assessments to support organisational and national partner agency understanding and activities. Significant partnership development and delivery is ongoing, including the following:

- Partnership working with Scottish Business Resilience Centre (SBRC) regarding Cyber Incident Response and developing expanded capabilities in relation to initial containment of Cyber incidents and response, investigation and recovery.
- We proactively engage with and produce positive investigative and preventative outcomes with a range of Scottish, UK and international partners, crossing the spectrum of public, private and third sectors. Our successes in dealing with online abuse, financial crime and reducing harm to the businesses and individuals relies upon, and benefits from, our existing relationships. Our partnerships are key to understanding and mitigating threats and to developing the joint capabilities through a Whole System Approach.

OFFICIAL

OFFICIAL

- Developing partnerships with the private sector, with a focus on preventing crime, minimising Cyber risks and supporting victims;
 - 'Web Ambassadors' have been established. Through an ever increasing network of organisations, the team are able to provide up to date information on threats/trends with mitigation advice. The network is supported by key organisations such Federation of Small Business, Chambers of Commerce, Business Improvement Districts and organisations in financial, oil, gas and energy sectors.
 - Cyber Scotland Partnership and Portal have been created. The Cybercrime Harm Prevention team have been instrumental in the development of a new partnership which has been formed to address the growing need for clarity on cybersecurity for individuals and businesses. The partnership is comprised of 10 strategic organisations across Scotland, including the SBRC, working together to ensure easy access to correct and up-to-date guidance on cybersecurity and resilience. The partnership is supported by the National Cyber Security Centre (NCSC), which joins as a technical advisor.
 - Relationships have been developed across the 'Protect Network'. As a key member of the protect network, collaborating with NCSC and Regional Organised Crime Unit's across England and Wales the team participate in national cyber security campaigns to support business; promote Cyber Essentials to improve cyber security and provide companies that have been victims of a cyber-attack expert advice on recovery and prevention. The team act as sponsors for suitable organisations to gain access to the Cyber Security Information Sharing Partnership (CISP). CISP is a joint industry and government initiative set up to allow UK organisations to share cyber threat information in a secure and confidential environment.
 - Improved internal and external communications have been established and will continue to be developed. Working with internal departments cyber prevention communications are devised, focused on building resilience across the business community. The team also participate weekly in providing content for the Scottish Government Cyber Bulletin, along with SBRC, SCVO and Trading Standards, highlighting threats/trends, case studies and training opportunities. The bulletin is circulated to public, private and 3rd sector across Scotland.

OFFICIAL

OFFICIAL

- Working in partnership with SBRC risks are being reduced to businesses. The team provide support to SBRC Cyber Incident Response and Exercise in a Box, providing organisations with tools and support to better protect themselves against cybercrime.
- Active support has been provided to Cyber Scotland Week and Safer Internet Day.
- 'Connecting Scotland' prevention activities are supported. The team have been involved in supporting the Scottish Government led Connecting Scotland Programme to support online safety and cyber security knowledge.
- We have worked in partnership with the National Crime Agency and Cisco to introduce a Digital Data Skills Academy (DDSA). This is a collaboration initiative between industry and Law Enforcement in order to deliver training for officers in a wide range of digital skills and will prepare our workforce over coming years to deal effectively with a range of threats and technologies.
- We have also conducted a refresh of our Probationer training programme with a focus on Policing in a digitally enabled age and equipped National Sex Offender Policing Units (NSOPU) officers with mobile triage devices in order to monitor offenders within our communities.

Over the next 12 months we will:

- Embed and strengthen our Partnership and Prevention approaches;
 - We will develop approaches to holistically and sustainably prevent cybercrime using partnership approaches;
 - We will identify areas to exploit partnership working and information sharing;
 - We will enhance links with the Scottish Education Cyber Programme and other relevant prevention programmes.
- Working with internal and external partners, we will strengthen our investigative capabilities to ensure that Scotland is a challenging place for cyber criminals to operate or affect.

OFFICIAL

OFFICIAL

- Through developing our processes we will ensure that they better support the reporting, investigation, and assessment of Cybercrime and support and reassure victims.
- We will work with internal and external partners to ensure that our focus on protection and safeguarding remains at the forefront of all we do and that we develop processes and partnerships to identify those at risk of online harm and methods to support early and effective intervention to protect vulnerable people and intervene in offending.
- We will further develop specialist roles i.e. PROTECT Officers, with a view to protecting minimising impacts on critical sectors across Scotland.
- Continue to develop an effective Cybercrime Intelligence Assessment through enhanced intelligence sharing, supported by partners in Law Enforcement and Industry.
- Continue to work with stakeholders and implement partnerships with Financial Institutions in Scotland utilising new, innovative and available technology to tackle online and organised fraud to protect individuals and businesses from the resulting harm.
- Support internal and external partners to proactively identify children and young adults vulnerable to exploitation from serious organised crime and work to ensure early intervention and appropriate diversification measures are implemented.
- Create capabilities and processes to ensure that Police Scotland is resilient and can respond to continually shifting Cyber threats.

OFFICIAL

ICT Cyber Security Strategy

We must be proactive in our approach to cyber threats. This includes within our own organisation and by providing support to the communities and businesses of Scotland. We will capture digital opportunities to keep people safe and enable Police Scotland, the public and organisations to proactively recognise and respond appropriately to cyber incidents. With that comes a requirement to build cyber resilience to prepare for, withstand, recover and respond to deliberate attacks or accidental events in the digital world. Police Scotland, with partners, supports resilience across all sectors, dynamically assessing the threat to the country, organisations, individuals and our own organisation.

The successful implementation of this objective will mean that Police Scotland is a cyber resilient organisation with the ability to continuously defend itself and others from digitally enabled harm, as well as working effectively with partners to support Scotland to be a cyber resilient country.

Aligned to, and supportive of wider Police Scotland Cyber Strategy, the ICT Cyber Security Strategy focusses on the delivery of a secure, resilient and future-proofed set of ICT deliverables. It will enhance the security of our data and robustness of our ICT systems.

The ICT Cyber Security Strategy will deliver a programme of work that will not only be an enabler for all the organisational strategic outcomes to be achieved, but will also enhance the overarching cyber security of the organisation and ensure Police Scotland remains a leading exemplar of cyber security within Public Sector in Scotland.

This is a multi-year programme, full details of which will be presented separately through established governance mechanisms.

Delivery will be against 5 key themes:

Assist

User education and awareness of cyber risk and issues is identified as a vital aspect of ensuring overall cyber security for an organisation. ICT will continue to work with relevant stakeholders to further develop the range of services available to officers and staff, in order to improve cyber security training material and guidance, such as good password management.

OFFICIAL

We will enhance hands-on training through interactive testing and perform cyber resilience exercises to simulate and prepare for cyber-attacks.

Detect

Data traffic inspection, security monitoring systems and management technologies will be implemented to detect threats and keep our data secure.

Assess

New, integrated approaches to performing internal security assessments and tests will be implemented and the Scottish Government Cyber Resilience Framework will be used to assess compliance and Cyber resilience across our infrastructure. Expansion of risk management techniques will occur to identify and mitigate risks and support governance reporting.

Protect

Current technologies will be enhanced and expanded to prevent unauthorised devices access to our network. Perimeter based protection will be enhanced to block malicious traffic automatically before it reaches the internal network and next generation anti-Malware tools will be implemented.

Transform

A progressive shift to utilising mobile and cloud technologies will commence, which will provide modern, scalable solutions in an efficient and innovative manner to support modern agile and flexible working, including using mobile applications. Authentication techniques will be enhanced to reduce risks of system compromise.

Locations and Assets

Estate requirements

Digital Forensics and Cyber Investigation currently operate from well-established sites nationally.

Work over the next 12 months will involve a review of processes and structures in these areas, both of which will define future estate requirements for Digital Forensics, Cyber Investigations and any emerging future structures. Any additional estate requirements and funding will be identified during the next year, with co-location opportunities being fully explored.

The establishment of Police Scotland as a Centre of Excellence sits at the heart of our ambitious Cyber Strategy.

Consideration is being given to the benefits of a virtual or physical Centre of Excellence, in conjunction with partners, to strengthen both Police Scotland and national capabilities. Scoping will continue during Phase 1 to assess existing service and partnership opportunities. Benchmarking is in progress with other UK agencies and this will inform the Design phase and production of implementation options. Associated structures, remit, capabilities and costs will be defined during this phase.

Demand Analysis

Demand Analysis

Challenges remain with accurate measurement of Cyber related data, given the complexity of related criminality and victimisation. The implementation of new systems, e.g. National Crime Unifi (COS) should improve the richness of this data but will take time to do so.

OFFICIAL

Work will be undertaken during Phase 1 of the Strategy Implementation Plan, in conjunction with the Police Scotland Demand and Productivity Unit, to enhance our understanding of Cyber demand to inform Design decisions.

We will progress activities to better understand the demand in order that our delivery of the Cyber Strategy takes into account changing trends and threats.

Development will focus on the following areas;

- User Journeys - Whole System Approach
 - We will develop our understanding of where our demand comes from, e.g. through monitoring crime reports and Cybercrime Tagged STORM Incidents - 2018 (333) rising to 2020 (6200).
 - Digital Forensics – we will measure caseloads and our performance in meeting public and Criminal Justice Sector partner demand.
 - We will develop insights to better understand available data to improve our responses and project future risks and demands.
 - Our approach will uphold our principle of employing a rights-based approach to policing, striking a balance between privacy and protection.
 - We will develop and enhance processes to improve user experiences and ensure that the needs of the wider Criminal Justice system can be met.
- When a greater understanding of demand is achieved, we will revise our resourcing approaches within Local Policing and Specialist Divisions and develop structures to support effective and sustainable service delivery, which will meet existing and future demand.
- We will continue to learn lessons learned from the progress already made e.g. digital triage, mobile devices.
- We will define and implement measures to enable relevant performance indicators to be applied and for success to be measured.

Information

Academic Research, Public and Community Engagement

In terms of academic research, Police Scotland will engage with relevant institutions during Phase 1 to establish strategic partnerships to deepen organisational and wider understanding of the Cybercrime threat, developing technologies and collaborative opportunities. We will consider creating MOU's and support appropriate access to Police Scotland information to support academic research and the development of innovative solutions to reduce victimisation and harm and enable more effective investigations.

Our approach to engagement and communication with the public, communities, partners and key stakeholders is a critical area of the work to implement the Cyber Strategy.

It is recognised that implementation of the strategy will require an open, transparent and ongoing conversation in Scotland to ensure our consideration of new policing is done with the consent of the public, to ensure the continued legitimacy of policing.

A high level approach to public engagement is being developed by the Programme team, supported by our Strategy and Innovation Department. The objectives of the engagement approach are:

- To be open, transparent and lead a wide reaching conversation on the development of new approaches to operational policing in a digital age.
- To continue to build trust and public confidence in policing, ensuring all appropriate parties are involved in new policing approaches to retain legitimacy and consent.
- To communicate effectively and address any public concerns openly as we implement our cyber strategy and the new approaches this will bring for the policing service in Scotland.
- To engage and collaborate with partners and key internal and external stakeholders, ensuring a cohesive evidence base to support decision making with the Scottish Police Authority and to offer assurance to Scottish Government and Parliamentary Committees.

OFFICIAL

Public engagement activity will be initially undertaken to align with Police Scotland's overarching engagement framework and the developing Cyber Implementation Plan to enable the right conversations on the key questions at an early stage. This will include the following:

- Creation of the first Citizens Online Panel for Policing in Scotland which will aim to be a representative, consultative body of the people of Scotland. The panel membership will ensure a representative demographic of Scotland and ensure appropriate representation of seldom heard groups. The Panel will enable a rolling programme of research and consultation over a 1-2 year period, including regular surveys and online discussions. This approach is recommended to enable effective engagement on the approaches in the Cyber Implementation Plan. It would be a positive, pro-active and dynamic approach for a policing service in the UK. The benefits include the ability to target specific groups, surveys and research can, if required, be undertaken at short notice and can track sentiments around policing approaches over a period of time
- Bespoke survey work to support the implementation of the cyber strategy will help the service to understand levels of public support and any areas of concern that can be addressed during service design and implementation. In addition, appropriate colleague engagement can also be undertaken to ensure effective support for our people.
- Focus groups will also be in place where there is a need for more in depth exploration of key areas with specific groups.

The insights from the research and engagement approach will test and enable the future design of policing services and approaches in Scotland, ensuring public consent is at the heart of all our considerations.

In addition, a range of partner and stakeholder engagements will be in place as the plan is implemented. This will include agreement of approaches with the Scottish Police Authority and, subject to the wider proposals for Police Scotland oversight and governance, setting up a Professional Reference Group with expertise from all sectors and academic contributions. The group will share best practice, leading research findings and provide both challenging and enabling collaboration as new approaches to policing are developed.

We will maintain and build our commitment to the recently formed Independent Advisory Group on the Police Use of Technology, chaired by Dr Liz Aston (Scottish Institute for Policing Research) and use this to build our understanding of public,

OFFICIAL

academic and expert views and opinions on the proportionate and effective use of data and technology to protect the people and businesses of Scotland.

Our engagement with the public in a way that informs our approach to delivering the Cyber Strategy is critical. We will seek to inform the public of the challenges that we face in this arena and to work with them to test how we could most effectively and ethically achieve our policing purposes of maintaining safety and wellbeing and tackling offenders, whilst prioritising fundamental Rights. We will seek to generate public debate and discussion and to make decisions around implementing practices and technologies which achieve the support of the public in order that we can achieve our objectives together.

We will also value the advice, scrutiny and challenge provided by the SPA and ensure that early dialogue occurs to both inform our developments and ensure that appropriate oversight exists on behalf of society as we operate in a digitally evolving policing environment that requires innovation, collaboration and new relationships with the public.

In addition to public engagement approaches, development of a communications plan for the programme and related work is underway.

Data

The Police Scotland Data Drives Digital Programme Full Business Case is currently progressing through internal and SPA governance. Whilst it sits outwith the remit of the Cyber Strategy this will compliment and support developments in investigating and preventing Cybercrime, including through introduction of Master Data Management, improved analytics capabilities and mechanisms to improve GDPR compliance.

During Phase 1 of the Cyber Strategy Implementation Plan work will be undertaken to assess and define existing and future Data requirements and the impacts of Cyber related business. Our understanding of Cyber threats should be enhanced via improved recording systems, e.g. COS UNIFI Crime, and enhanced data sources.

We will collaborate with the Data Drives Digital Programme to explore how the ethical use of data could improve our response will ensure that all activities are in accordance with the introduction of our new Data Ethics Governance Framework.

This will provide additional internal and external scrutiny of 'data-driven technology' projects.

Organisation

Strategic Workforce Planning

The first phase of the Police Scotland Strategic Workforce Plan (SWP) has been approved by the SPA, with Divisional plans making repeated reference to Cybercrime demand. Some plans highlighted intentions to begin work on the development of teams and local strategies, however the remit regarding local work in the Cyber space was made clear in terms of the imminent publication of the overarching Cyber Strategy. It was agreed that more detailed plans would follow the implementation of the Strategy.

The first quarterly update from local areas was due recently, the contents of which will be reviewed in relation to the Cyber Strategy objectives and priorities.

In recognition of existing demand and capacity within Digital Forensics, Cyber Investigations, Intelligence Support and Cyber Harm Prevention agreement has been reached within Police Scotland that 40 Police Staff posts will be assigned to these business areas within Phase 1, without additional overall staffing costs being incurred through re-investing capacity created elsewhere. Consideration is currently being given to assigning a further 34 posts in Year 2 via the same means. Further demand work to be undertaken as part of Phase 1 which will inform such decisions.

During Phase 1 of the Implementation Programme, the Strategic Workforce Planning Team will provide support and guidance at appropriate stages, focussing on the following areas;

- Training in the 6-step methodology for teams or individuals who will be determining future workforce requirements;
- Provision of templates to complete an outline workforce plan, and supporting current and historical data from SCoPE relating to any identified sections of the existing workforce;
- Support sessions to assist the work on creation of a draft plan;

OFFICIAL

- Draft review process,
- Assistance with how to structure the ongoing review and monitoring process for the plan

The Cyber Strategy Implementation Programme will liaise closely with related business areas and design Boards to ensure that all relevant SWP activities are undertaken. The focus of activities will initially be on defining Centre of Excellence, Digital Forensic and Cyber Investigation requirements. Demand analysis will also influence discussions around Local Policing and Specialist resource profiles.

Capability and Training

A Cyber and Digital Training and Development sub-group consisting of individuals from various training and operational areas has been established and this group is currently conducting a Training Needs Analysis (TNA) to establish what training and development products are currently available to Police Scotland officers and staff and to define the current "as is" position in terms of skills across the organisation in terms of Cybercrime.

On completion of the TNA and identification of gaps, work will be undertaken during Phase 1 to identify solutions, including through benchmarking.

Whilst the outcomes of the TNA are currently not fully known the following outcomes are anticipated;

- It is estimated that operational officers and staff (c. 11,000) will require upskilling, most likely through online learning on a modular basis.
- Generalist Investigators (c. 3,000) are likely to require specific additional module(s) which may be delivered through blended learning (online/classroom).
- Specialist investigators (c. 400), including those assigned to Cybercrime, Internet and Communications Investigations, along with Intelligence Officers, are likely to require specialist training on an initial and ongoing basis. This is likely to be blended approach with varying abstraction needs for mainly external training.

OFFICIAL

It is likely that training products will require to be either developed internally, or procured externally (likely given specialist knowledge required). The content and duration is expected to vary according to role and required skills.

Timelines for Delivery (Phase 1)

Enablers Police Scotland Resilience – Design Begins		Enablers Cyber/ Digital Crime Capability – Build Capability		Enablers Private Partnerships – Private Partnerships with Financial Institutions		Enablers Cyber/ Digital Crime Capability – Build Capability	
Q1 2021 (Apr May June)		Q2 2021 (Jul Aug Sept)		Q3 2021 (Oct Nov Dec)		Q4 2022 (Jan Feb Mar)	
Initiation		Implementation				Delivery	
Customers and Demand Discussions between Cyber and DPU Teams on Approach to Demand Data	Academic Research and Public & Community Engagement Bespoke Survey Further Meeting to Survey and Determine Milestones	Customers and Demand Work with DPU to assess Demand	Training & Development Capability Build and Development of Key Products	Training & Development Align Requirements to Centre of Excellence Design	Data Target Operating Model Rollout Complete (Nov)	Customers and Demand Review with DPU	Customers and Demand Report Findings
Academic Research and Public & Community Engagement Citizen's Panel Initial Discussion with the Cyber Team	Academic Research and Public & Community Engagement Focus Groups Further Meeting to Survey and Determine Milestones	Academic Research and Public & Community Engagement Citizen's Panel Establish Engagement Mechanisms		Strategic Workforce Planning Engage SWP to Support the Development of the Workforce	Data Master Data Management Project End (Nov/Dec 2021)	Data GDPR Project End (Jan/Feb 2022)	
Academic Research and Public & Community Engagement Bespoke Survey Initial Discussion with the Cyber Team	Data Target Operating Model Consultation (May)	Data Data Ethics Governance Framework Rollout of Data Ethics Governance Framework				Data Force Wide Analytics Project End (Jan/Feb 2022)	
Academic Research and Public & Community Engagement Focus Groups Initial Discussion with the Cyber Team	Data Target Operating Model Rollout Commences (June)	Training & Development Align Requirement to Centre of Excellence Design				Locations & Assets Governance & Delivery	
Data Target Operating Model (Apr 2021)	Data GDPR Project Start (May/June 2021)	Training & Development Decide on Internal/ External Provision				Training & Development Phased Implementation of Delivery and Evaluation of Products	
Data Master Data Management Project Start (Feb 2021)	Data Data Ethics Governance Framework Police Scotland Approval (May 2021)	Strategic Workforce Planning Initial Awareness Session with Cyber Team					
Data Force Wide Analytics Project Start (Apr 2021)		Strategic Workforce Planning 6 Step Methodology and SWP Overview Training					
Locations & Assets Design		Strategic Workforce Planning Design Opportunity to discuss the SWP input to Centre of Excellence					
Mobilisation, Design and Delivery Resource Requirements – Team in Place							
Training & Development Scoping and identification of Products/ Key Resources put in place							

OFFICIAL

Successful delivery of this ambitious strategy will involve managing complex dependencies and risks.

Dependencies

A range of internal dependencies have been identified, centred on related strategic change programmes within Police Scotland;

Digitally Enabled Policing Programme	Crime, Intelligence and Case Reporting systems.
Contact and Engagement Model (CAM2)	How we engage with members of the public, including those who wish to report Cybercrime or seek advice in relation to it is a significant part of the Cyber Strategy delivery. During Phase 1 we will work with CAM2 colleagues to develop modern means of engaging with the public, as well as enhancing Cybercrime skills and knowledge within this business area.
Digital, Data and ICT Strategy	Delivery of the Cyber Strategy is dependent on the delivery of a range of technologies, e.g. infrastructure, software and the Cyber Security Strategy.
People and Development	Strategic Workforce Planning and Leadership, Training and Development.
Digital Evidence Sharing Capability Programme (DESC)	We will work with the DESC Programme to develop means by which digital evidence (including high volume) can be appropriately stored and shared, including with Criminal Justice Sector partners.
Intelligence Review	Development of revised Police Scotland approach to intelligence management, including Cyber related.
Local Policing Review	Shared dependencies regarding Cyber capabilities and capacity building to improve public service.

Risks

Partners	Strategy implementation will rely on the support and co-operation of a range of internal and external partners, including those in public, private and voluntary sectors.
Availability of finance	We are operating in a period of significant financial constraints and competing

	demands for funding. Capital funding availability means that we will require to prioritise projects that deliver the most benefits earlier, and forward plan to deliver projects as and when further funding resources become available.
Technology	Achieving our ambitions in relation to Cybercrime will require significant investment in technology and adoption of new processes. Public views, as part of our Rights based approach, will influence the extent to which we may adopt new and emergent technologies.
Resources	Competing demands for human resources may affect delivery of the change, including the availability of those with specialist skills.

 **Management**

Finance

Financial planning will occur in line with established Programme governance and Business Case processes.

Known and approved costs for FY 21/22 have been included below.

It is anticipated that the Design phase will identify further Capital and Revenue requirements, the majority of which will be required to support delivery in future financial years. At present, the most likely additional requirement this year will relate to the provision of skills and learning enhancement, which is likely to be identified through an ongoing Training Needs Analysis. Whilst finances are currently committed to this element of the Programme during this financial year, decisions may be needed as to whether additional funding requirements are met this year, or deferred.

OFFICIAL

Total cyber spend budgeted in 21/22 (£'s)	Total spend by category (£'s)
Split as per the following category's	
Op Urram 100,382	Op Urram (revenue) 100,382
Cyber Capabilities 1,088,029	Capital 751,757
Cyber Strategy 1,081,934	Reform 1,126,803
Cyber Security Implementation Plan 639,678	Revenue 931,081
Total spend budgeted in 21/22 £2,910,023	Total spend budgeted in 21/22 £2,910,023
Additional 40FTE staff requested to be found from within existing police Scotland staffing budget through reprioritisation £923,685	40FTE staff - Revenue to be found from within existing police Scotland staffing budget through reprioritisation £923,685
Additional 5FTE ICT Cyber Security staff £272,541	Additional 5FTE ICT Cyber Security staff £272,541
Total anticipated 21/22 spend £4,106,249	Total anticipated 21/22 spend £4,106,249

ICT Cyber Security costs for FY 22/23 are currently projected to be £1,183,592 (budgeted), including £541,914 in relation to an additional 10FTE Cyber Security staff.

This currently includes £448k assigned to the Cyber Capabilities Programme for training purposes. Should the outcomes of the ongoing Training Needs Analysis be supported it is currently anticipated that overall training costs of c. £2.25m (plus abstraction costs) will be required in Phase 1 (not currently budgeted).

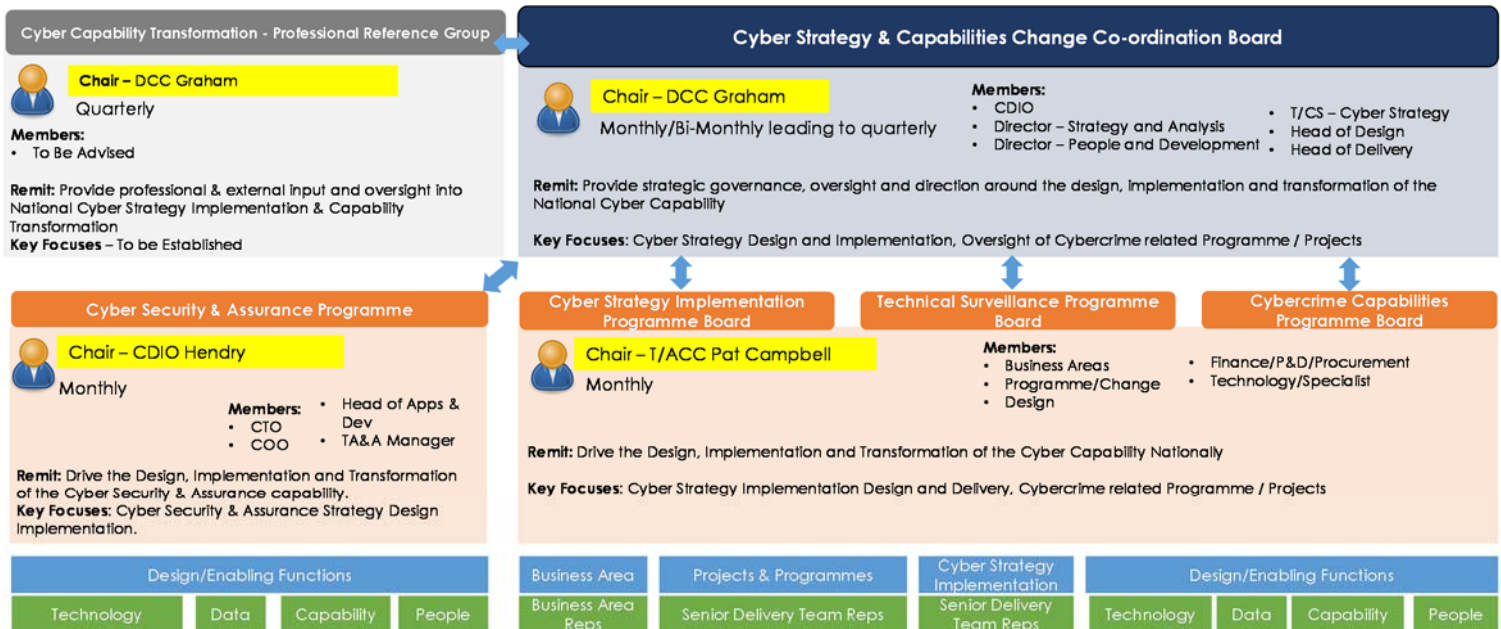
Governance and Oversight

Relevant governance and oversight arrangements have been implemented, overseen by DCC Graham (Crime and Operations) as Executive Sponsor and Chair of the newly established Cyber Strategy & Capabilities Change Co-ordination Board.

Reporting via Project and Programme Boards will occur, as per established practice, overseen by ACC Pat Campbell (Organised Crime, Counter-Terrorism and Intelligence) as SRO for the Cyber Capabilities and Cyber Strategy Implementation Programmes and CDIO Andrew Hendry as SRO for the Cyber Security and Assurance Programme.

Regular reporting on progress of the implementation will be provided to the Police Scotland Change Board, Corporate Finance and Investment Group, and Strategic Leadership Board.

Police Scotland will also report progress to the Scottish Police Authority to the appropriate committee and the Authority Meeting, as required.



Professional Reference Group

As outlined above, formation of a Professional Reference Group chaired by DCC Graham and involving a range of external specialist stakeholders, will engage and involve interest groups and specialist communities in the design and development of our approaches, inform our wider community engagement and consultation and support our objectives of keeping people safe in the digital world, through the ethical use of modern technologies.

The group will also support and empower our development of effective partnerships and preventative initiatives, influence our approach to further embedding a Rights based policing model and inform dialogue with wider democratic forums on the legitimate use of technology to enhance national policing services.