New Zealand POLICE
Nga Pirihimana O Aotearoa

Information and Systems Strategy and Roadmap

2013–2018

November 2013

New Zealand Government

Contents

Preface

New Zealand Police seeks to be at the forefront of policing internationally, demonstrating the hallmarks of a modern Police service: Innovation, agility, visibility and transparency. We are building an organisation that is 'fit for purpose' in an increasingly sophisticated world. In doing so, we recognise the imperative of maintaining a high level of public trust and confidence in Police.

Information is the life blood of modern policing and mobile technology makes it easier for our officers to access and share information. When our officers have easy access to timely, relevant information they are far better placed to prevent crime and road trauma. They can also respond more promptly and resolve crime and road trauma more quickly.

Over recent years we have increased our focus on the use of information and the systems that provide it. A major driver has been the Policing Excellence programme, which has at its heart an operating strategy Prevention First. By its very nature, this operating strategy works effectively when our officers have the right information at the right place and time.

I believe that New Zealand Police can be world class in the way it applies technology to policing. I have challenged our ICT Service Centre to be more innovative in finding solutions that improve policing. This has led to a number of initiatives, such as communications centres and mobility, which are now recognised as global references for good practice. But more importantly these initiatives are increasing productivity and improving community safety.

The ICT Service Centre has been transforming the way it works – its charter focuses on innovation, positivity and partnership. Given the complexity of the world in which we operate, collaboration is more important than ever. The ICT Service Centre needs to work in partnership with suppliers, other government agencies and critically, with the operational parts of New Zealand Police.

In the management of its information and systems, Police needs a clearer long term direction, linked strongly to the Police National Strategy. This document provides that direction by translating long term operational policing needs to roadmaps for improving information management and the development of our technology systems. It takes a five-year perspective, which is brave thing to do in these times of rapidly changing technology. But I am confident that the direction set will serve us well by informing strategic investment and supporting key operational decisions.

Therefore, I endorse the Police Information and Systems Strategy and Roadmap 2013–2018.

Viv Rickard

Deputy Commissioner, New Zealand Police

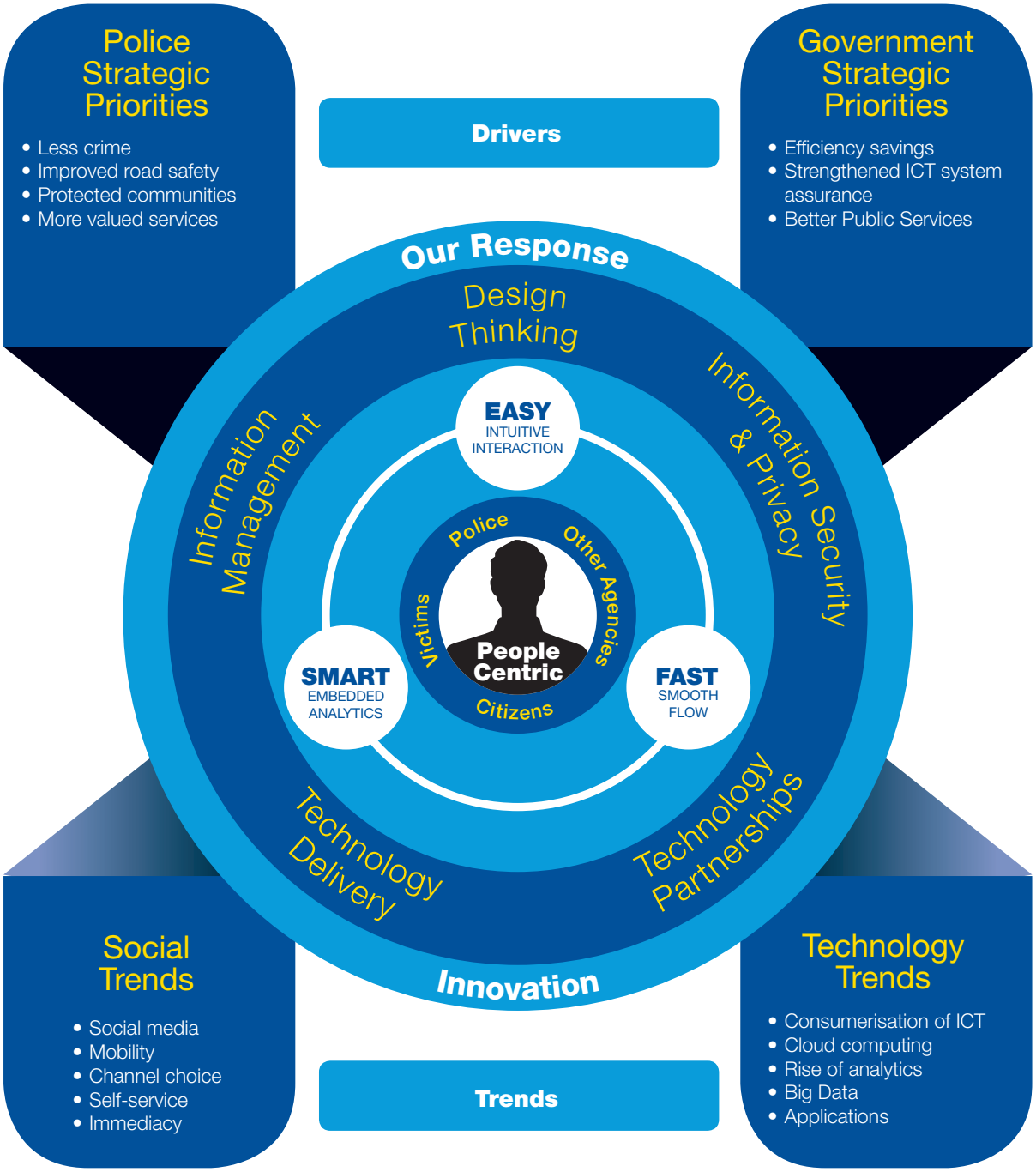


Figure 1: Police Information and Systems Strategy and Roadmap – Context and Direction

Part 1: Strategic Direction

Purpose

This Information and Systems Strategy and Roadmap (ISSR) provides strategic direction for the development of information, processes and ICT systems at New Zealand Police. The strategic direction, informed by Police National Strategy, places information users at the centre of Police information management. This clear direction will ensure Police's information needs drive the development and management of our ICT systems.

Approach

Police's response to the information and technology landscape of today was to first recognise its influence on our own operational context. Having noted that influence, we began by establishing appropriate information governance to ensure that the ISSR would be owned by Police operations and not simply amount to an IT-oriented plan. That governance, including Police's information principles, is explained in more detail later in this Part 1.

A programme of work was then undertaken with the information domain owners to develop information domain roadmaps. These roadmaps individually provided direction for each information domain, and collectively revealed common themes across Police needing their own statements of direction, for instance geospatial information. ICT Service Centre management and technical experts were also engaged early on in a workshop to help frame the ISSR and to anticipate implications for the ICT delivery plan.

The future direction of Police's information and systems has been informed by this work and is presented and explained in the following terms:

- **Strategic Direction:** Focus on people's information needs, to make information services Easy, Smart and Fast
- **Foundational Capabilities:** The fifteen capabilities we need to achieve our strategic direction
- **Enablers:** The five areas we need to focus on to realise the foundational capabilities:
  - Information Management
  - Information Security and Privacy
  - Design Thinking
  - Technology Delivery
  - Technology Partnerships
- **Police Information Roadmap:** Shows the current and future information landscape at Police, along with a series of Information Roadmap (IR) priorities.
- **Police Systems Development Roadmap:** Shows the current state and future state systems models, with associated Systems Development Roadmap (SD) priorities.

Context

Police strategy, social trends, technology trends and Government ICT Strategy provide the context for this ISSR. See Figure 2.

Figure 2: Strategic Context

Police Strategic Priorities[1]

Police's vision of 'safer communities together' is enduring and signals our mission 'to work in partnership with communities to prevent crime and road trauma, enhance public safety and maintain public order'. Our objectives of 'be safe, feel safe' summarise the long term outcomes Police seeks, which are 'confident, safe and secure communities' and 'less actual crime and road trauma'.

Our strategic priorities are:

- **less crime:** reduced recorded crime
- **improved road safety:** reduced hospitalisations from road crashes
- **protected communities:** reduced repeat victimisations
- **more valued services:** maintained trust and confidence in Police.

The Police Model, with its twin pillars of Prevention First and People and Victim Focus, and its emphasis on continuously improving support to frontline Police staff, provides the operational focus to implement our strategic priorities.

1 New Zealand Police Strategic Plan 2011-2015, New Zealand Police Statement of Intent 2013-2015 p12

Government Strategic Priorities

As part of its drive for efficiency savings, the Government expects information and technology to be used to deliver better services with sustainable business savings of $100 million per year by 2017.

The 'Government ICT Strategy and Action Plan to 2017' aims to deliver the required savings and improvement in service delivery. The Strategy focuses on transforming service delivery through digital self-service channels, and proposes moving away from an owner/operator model for technology assets in favour of a services-based one. It envisages the future of government ICT as information-centric rather than technology-centric. Finally, it seeks to strengthen ICT system assurance to manage risk and quality.

The Strategy is supported by an Action Plan with four integrated focus areas: services are digital by default; information is managed as an asset; investment and capability are shared; leadership and culture deliver change. System assurance activities are not a separate focus area. Rather they are integrated into each of the four focus areas.

The Strategy reinforces the Better Public Services programme by requiring agencies to look beyond their own priorities to public sector priorities. The Government has set ten challenging results in five areas for the public sector to achieve over the next five years. Result 10 – New Zealanders can complete their transactions with the Government easily in a digital environment – falls under the area of 'Improving interaction with government'. The target for Result 10 is an average of 70 percent of New Zealanders' most common transactions with government will be completed in a digital environment by 2017.

State Services agencies are expected to align their plans with the Strategy and Action Plan. This ISSR achieves that alignment with the Strategy and with Result 10 (See Appendix 2).

Social and Technology Trends

Police is experiencing an accelerating transition to a digital information-based operation, and overall global trends will continue to have significant implications for how Police operates in the future.

The popularity of social media has made immediacy, channel choice and self-service the currency that really counts when people communicate and engage online. The rapid adoption of feature rich, easy to use mobile devices is changing the way people access the internet and digital services. This consumerisation of ICT means that time and place are no longer barriers to accessing digital services.

Network providers are delivering faster internet access to end-users that will allow more and richer services to be delivered through the digital channel. This trend is reflected in the Government's Ultra-Fast Broadband Initiative for wired networks as well as improvements in mobile networks.

Cloud computing represents a changing business model where highly scalable services can be purchased without the need to invest in the underlying hardware and software. The Government's approach to the cloud means that agencies, including Police, will be expected to move away from existing business models and embrace cloud-based services.

The rise of analytics, taking advantage of increasing computer power and the information explosion referred to as Big Data, is transforming intelligence work. For example, analytics can be applied to predict trends in performance and demand, understand causal relationships, develop and validate risk assessments, and recognise data from different sources as relating to the same instance or person.

The pervasiveness of mobile devices is a key driver of the trend away from complex applications that need extensive training, to applications that focus on specific interactions within business processes, intuitively guiding users and requiring minimal training.

Police Strategic Direction – Place People at the Centre

People before Systems

Police is responding to the above drivers and trends with a fundamental shift in thinking, moving from a system-centric approach to a people-centric one. In particular, the rapid uptake of mobile devices and information services has proven that placing people at the centre of process, information and systems design is fundamental to success.

Innovation

With people in the centre, we will be innovative in developing our information systems to meet new requirements. We will use new ideas and methods in ways that support our mission. In this way, we will not only strive for incremental improvement, but we will continually assess whether different approaches will deliver better results.

Model for Process, Information and Systems Development

At the heart of our strategy are people – the victims, citizens, Police staff and staff in other agencies – who interact with us. They are the people with whom we work in partnership in pursuit of our vision of Safer Communities Together. We will focus on the information needs of these people. The focus on people and the application of our Information Principles will guide the development of processes, information and systems.

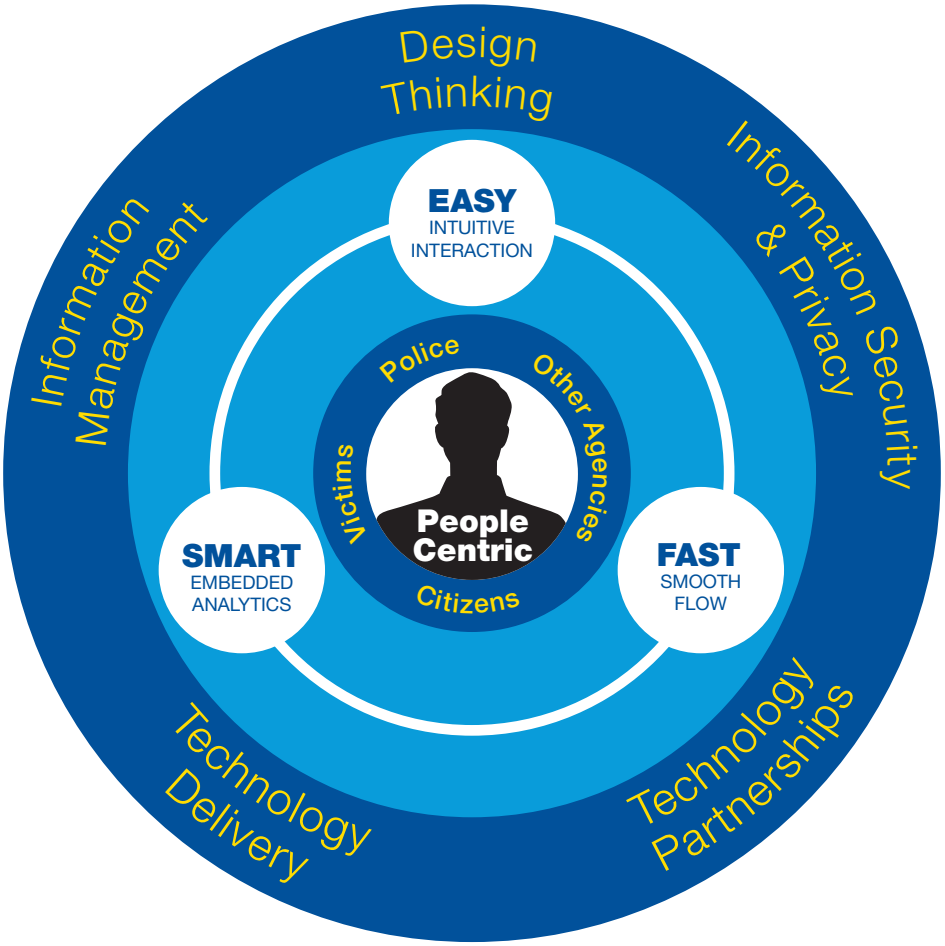


Figure 3: The Police Information Model

People can expect their interactions with us to be easy, smart and fast (see Figure 3):

Easy: Interactions will be intuitive. They will make sense in the context in which they occur and will require little training or guidance. People will choose the channel that suits them best.

Smart: Analytics will be embedded in our systems and processes to support all users. Analytics will combine historical and predictive analysis to provide insights and support decision-making.

Fast: Processes will flow smoothly for people. Information will flow to and from wherever it is needed with minimal human intervention. Automated workflow will join processes to deliver services efficiently.

Foundational Capabilities

To make things easy, smart and fast for people we need to consider the vital few capabilities which need to be in place to deliver on this strategy. Each characteristic of people's interactions with Police information and systems – easy, smart and fast – will be supported by five foundational capabilities, which are shown in Figure 4. Each capability and its direction is described below.

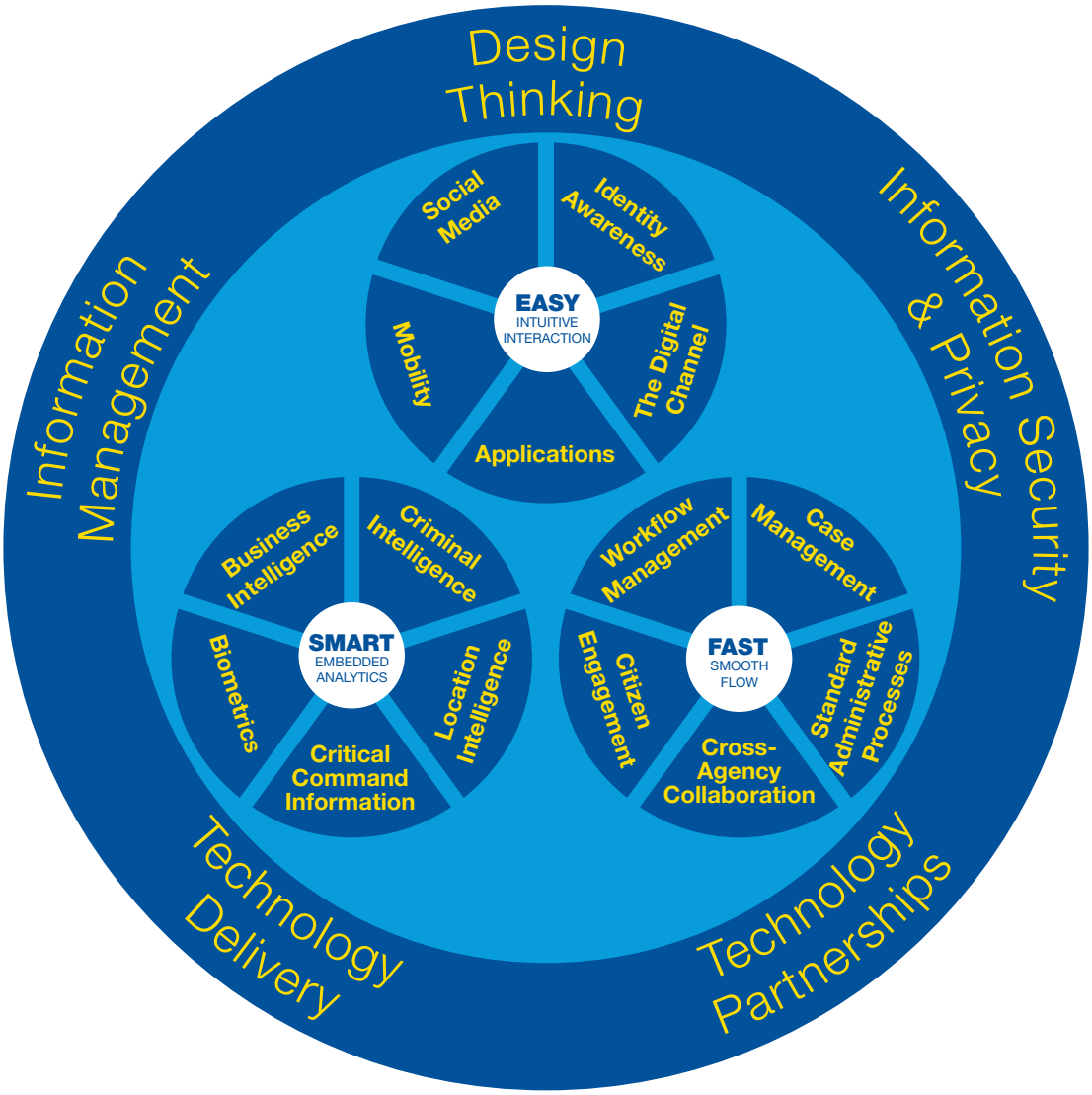
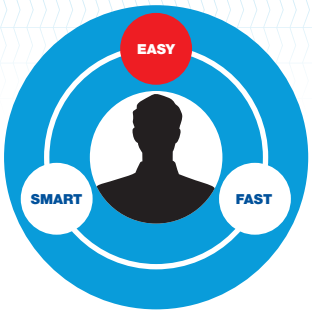


Figure 4: The Police Information Model showing the 15 Foundational Capabilities and the 5 Enablers

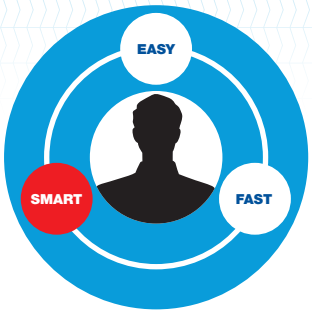


Intuitive Interaction – Making It Easy

Intuitive interactions make it easy for people to do the things they need to do. The way in which people engage with information, the processes they use and the types of devices they prefer has dramatically shifted and will continue to shift over the next five years. We need to put in place fundamental capabilities that adapt to preferences and ensure that people spend the minimum time getting to the information they need.

FOUNDATIONAL CAPABILITY	DIRECTION
FC1 — Social Media	Adopt social media approaches to enhance communication and collaboration, increase real-time engagement and improve ease of use. Internally, adopt social media approaches so teams can exchange information, collaborate and stay informed. In the public domain, adopt a cohesive social media presence to meet the public's expectations of easy interactions with government.
FC2 — Identity Awareness	A user's identity will be used to personalise their interactions with Police information systems. Identity awareness will allow users to customise interfaces to organise information and functionality, ensuring a consistent experience across applications and devices. People can use RealMe to interact with Police services online e.g. reporting non-urgent crime and lost property, or finding out the status of a case in which they are involved as a victim or witness. People will still have the option of reporting crime anonymously. Identity verification for Police staff will be role-based to ensure it appropriately underpins information access and security. Police will work collaboratively with other agencies to develop and use agreed standards for identification in the Justice Sector. Agreeing the same terms to identify offenders will make using information shared across the Justice Sector easier and more intuitive.
FC3 — The Digital Channel	Police will increasingly take advantage of the digital channel to give the public a more seamless experience when using services provided by Police and wider government. In doing so we will also be supporting Result 10. Where appropriate, Police will use the digital channel to deliver services, allowing the public to interact with Police in the way that suits best, including self-service and real-time interactions.

FOUNDATIONAL CAPABILITY	DIRECTION
FC4 — Applications	Police will take advantage of simpler end-user applications to make services available, for Police staff, and for the public through the digital channel. This follows the trend away from complex applications that need extensive training, to applications that focus on specific interactions within business processes, intuitively guiding users and requiring minimal training. Where appropriate, we will use rapid application development techniques. Applications will be delivered across devices and operating systems to best fit the requirements (whether via native applications or web browsers).
FC5 — Mobility	In conjunction with Applications and the Digital Channel capabilities, Mobility will make all Police information and services available from anywhere at any time. This will be assisted by increasing data bandwidth available in mobile networks, such as 4G and beyond, allowing richer and faster content delivery. When they can, all staff will work without a dedicated desktop computer. All services for the public will be designed to be mobile from the beginning so they can have the best possible experience in their interactions with Police.

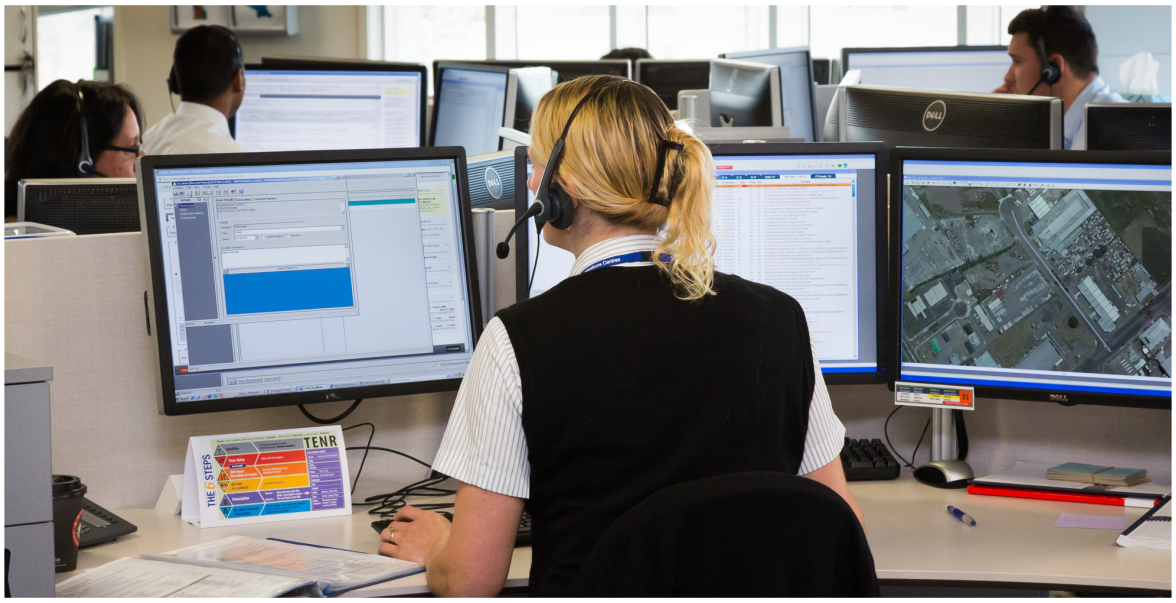


Embedded Analytics – Making It Smart

Embedding analytics within our systems and processes speeds up decision-making. Automated information processing means staff will spend less time analysing and interpreting information and more time acting on it. We will make good use of sensors, pattern detection, monitoring and notifications to enhance intelligence. We will explore the use of expert systems that draw on applied knowledge to support decision-making.

FOUNDATIONAL CAPABILITY	DIRECTION
FC6 — Business Intelligence	Business Intelligence (BI) allows Police staff to analyse, measure, predict and report on key policing metrics. It improves accuracy of statistical information and helps to identify trends and emerging issues. BI also contributes to higher quality inputs for key planning processes and puts consistent performance information in the hands of the decision-makers who use it. The BI environment may contain more than one data repository. However, Police will standardise where data is sourced, to ensure consistent, trustworthy and authoritative information. We will take advantage of developments in business analytics technology to perform predictive analysis within the BI environment, to reduce the work required by analysts, and to deliver timely information directly to decision makers through simple, easy-to-use interfaces. Police will make high quality, valuable information such as crime statistics (including crime volume forecasts) increasingly open and available to citizens through the digital channel.
FC7 — Criminal Intelligence	Criminal Intelligence allows Police to analyse data to provide understanding and insight into the links and relationships between people, location, entities and crimes. It provides a real-time view of the criminal environment to the Police frontline, and as such is at the core of Prevention First. The use of in-depth intelligence products helps to identify emerging crime problems and reduce crime. A predictive analytics platform, spanning internal and external data sources, will make links between data, and identify critical intelligence information. Increased use of automated information feeds and alerts will improve dissemination of intelligence information. Real-time sharing of information with other agencies will allow dynamic risk scoring of offenders or people at risk. Serious crime investigation will be enhanced by the use of entity extraction, predictive analytics, data mining, location mapping and data visualisations. In the field, officers will have the ability to link the queries they make, for instance, about a person or about a vehicle, to improve the quality of intelligence information.
FC8 — Location Intelligence	The majority of policing information has an associated location, and mapping is often the only way to make sense of large amounts of data. Capturing, analysing and presenting location information provides unique insights into the crime and crash environment. Seeing the location and capability of Police resources in real-time allows for better deployment decisions and helps to keep officers safe. A range of location services will be available through a standards-based geospatial environment that complies with the NZ Government Geospatial Strategy. These services will include mapping, routing, standard boundaries and geo-fencing, and will be available to our users directly and also via other systems. Maps will have a common look and feel regardless of the application they are accessed from or the device used. All location intelligence across Police will be standardised to ensure consistency and promote a common understanding. The geospatial environment will act as a hub from which Police will make use of data sources provided by third parties and layer them to see and understand patterns. It will allow Police to share analysed location information with other agencies and to share crime and crash statistics with citizens through the digital channel.

FOUNDATIONAL CAPABILITY	DIRECTION
FC9 — Critical Command Information	Critical Command Information will be integrated and presented across Police (and potentially other emergency services) through a common interface to provide a common operating picture. All command decision-makers will have access to the same authoritative information regarding resources and demand for service in and across Police districts. This will allow District Command Centres to coordinate command decisions across a district to achieve district priorities. A clear understanding of available Police resources (actual strength) and of current and planned activities across all workgroups and external partners will lead to improved tasking and coordination. Information will be presented from multiple systems inside and outside Police, including texts, photos, videos and live feeds captured in the field through mobility devices. Frontline staff will be able to access up-to-date information on victims, offenders and locations of interest while they are dealing with them in the field.
FC10 — Biometrics	The capture and analysis of advanced biometric information in the field using mobility devices – superior palm and fingerprint matching, facial recognition, electronic capture and searching of tattoos – will help frontline Police prevent crime, reduce victimisation rates and successfully identify and prosecute offenders. Whenever possible biometric capabilities will use an integrated multimodal approach – using a number of biometric identifiers – to provide a single set of biometric information for capture and searching.



Smooth Flow – Making It Fast and Efficient

When people deal with Police – whether as a member of the public, a victim of crime, someone from another agency, or as a member of Police staff – the processes they use need to work smoothly, end to end. They should be able to interact or transact with Police with a minimum of effort, saving them time and saving Police resources. The smooth flow of information and processes increases satisfaction by ultimately delivering better results.

FOUNDATIONAL CAPABILITY	DIRECTION
FC11 — Workflow Management	With improved workflows Police staff will be able to access and capture information more quickly. Electronic forms used for these purposes will incorporate business rules which will operate dynamically based on the information entered. Those on the frontline and those investigating crime will be better informed and will spend less time completing essential paperwork. Staff working in the field will use their mobile devices to seek information from Police systems and also to capture information for those systems. The information will be more accurate, because it will be verified at the point of capture. Information will be transferred electronically to Police systems, reducing processing time, and it will be easily retrieved because it will be associated with the event to which it relates.
FC12 — Case Management	Cases will progress quickly and smoothly, with standardised processes being supported by electronic workflow. Irrespective of the devices and channels used, workflow initiated in the field as part of case management will be progressed in our File Management Centres. Documents and other digital assets (such as photos and video) relating to a case will be stored in a central repository, and linked from within systems that need to refer to those files. In this way all information relating to a case will be readily accessible from one place. Electronic workflow within case management will allow Police to continue improving services for victims of crime, ensuring they are kept well informed by Police staff or through self-service via the digital channel as the case progresses. Building on the electronic filing of charges and bail applications with the Courts – under the Electronic Operating Model (EOM) – working with the Courts will be completely electronic.
FC13 — Standardised Administrative Processes	Administrative approval processes in areas such as Human Resources and Finance will require minimal effort. Electronic workflow – with smart forms where practical – will be embedded in these support systems to replace manual paper-based processes, reducing errors and improving processing time. Use of staff self-service for matters such as expense claims will save time, and administrative reporting will be improved through the availability of more accurate information.

FOUNDATIONAL CAPABILITY	DIRECTION
FC14 — Cross-Agency Collaboration	Information will be easily and securely shared between Police and other government agencies and partners. The public dealing with government will get the best seamless experience through effective cross-agency collaboration. In addition agency performance will be improved through mutual information sharing (e.g. real-time intelligence) with other agencies in New Zealand and internationally. Automated information exchange with other agencies will be based on standardised approaches to information management and sharing.
FC15 — Citizen Engagement	Engaging well with the public engenders trust and confidence. Engagement with communities, neighbourhoods and other groups is also an important aspect of crime prevention and resolution. The public will be offered multiple channels so that they can choose to engage with Police in the way that suits them best. Services that include public interactions will be designed around the public, with other agency and Non-Government Organisation (NGO) services linked into the process as required.

Enabling the Strategic Direction

The foundational capabilities will be delivered and integrated by effective information management, information security and privacy protection, the use of design thinking, the delivery of technology and the development of technology partnerships.

Enabler 1: Information Management

Police Information Principles

The following are Police's Information Principles, which are based on the Justice Sector Information Principles. They provide the foundation for effective information governance and planning at Police.

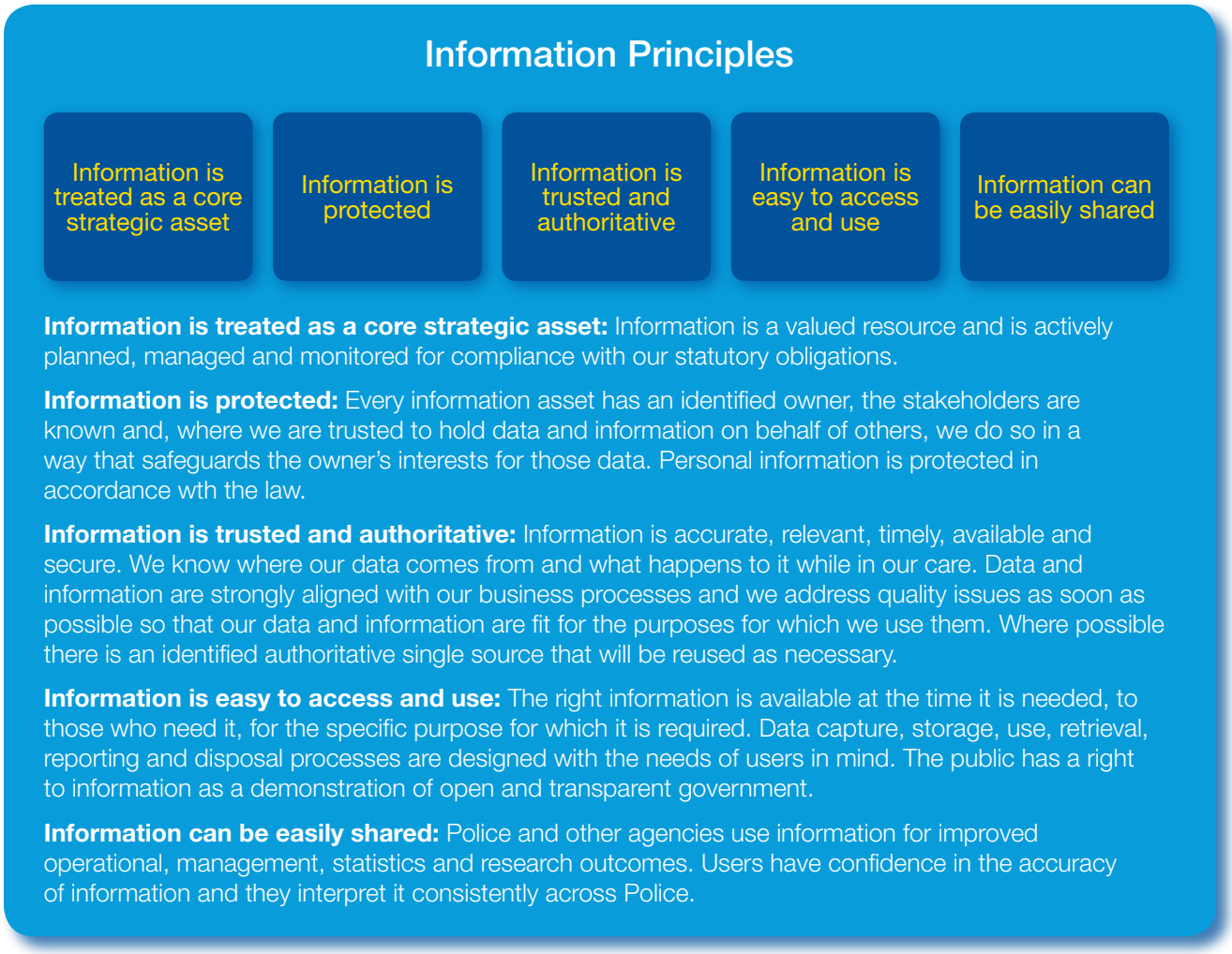


Figure 5: Police Information Principles

All initiatives, projects and programmes will follow the Police Information Model – Easy, Smart, Fast – and will be required to demonstrate adherence to the Information Principles from the outset.

Information Governance

The Police information governance structure ensures effective decision making through the Commissioner of Police and the Police Executive, and engagement of relevant business owners across Police. The Commissioner approves the Police National Strategy, which informs the ISSR and the ICT Delivery Plan, both of which are approved by the Police Executive.

The Police Information Management and Security Committee (PIMSEC) is tasked on behalf of the Police Executive to coordinate the planning of information and security risk management. PIMSEC endorses the ISSR for Police Executive approval. It also reviews and endorses information plans and directions, and provides advice to the Police Executive, the CIO and Police business owners on matters relating to information security risks and the effective use of information within Police.

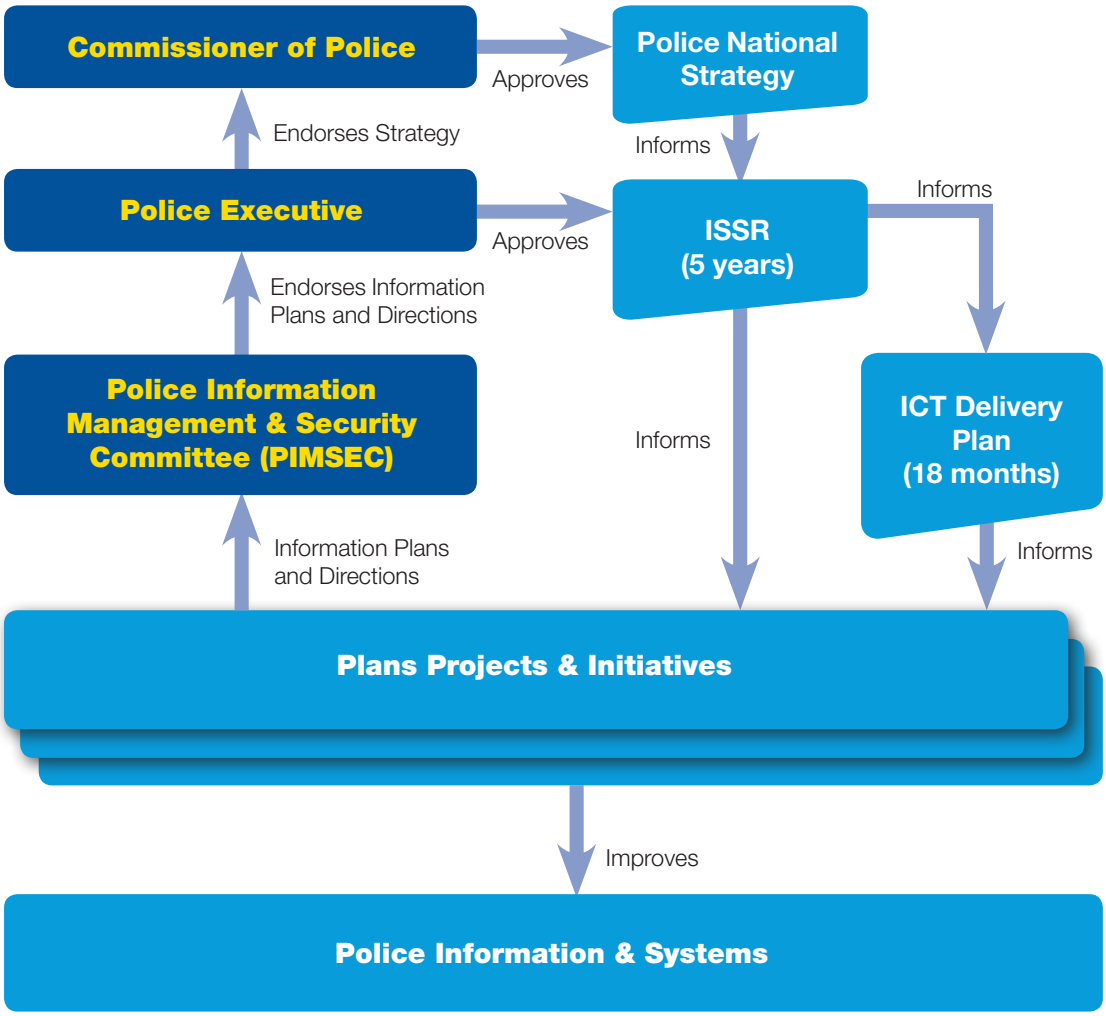


Figure 6: Police Information Governance

A pre-requisite for people-centric information systems is a clear understanding of the breadth and depth of Police's information needs. This is achieved by bringing together people representing various information domains to consider Police's information strategy and plans. These information domains link to Police operational units and are expected to evolve over time.

Each information domain has an owner, whose role is critical to the delivery of effective information systems. The domain owners are people with detailed knowledge of the business processes and information within their domain who are sufficiently senior to take accountability for the information and data quality, integrity and security within their domain. This ensures that our strategies and plans are owned by Police operations, and are not simply IT-oriented.

Collectively the domain owners, supported by Police information professionals, work together on PIMSEC to shape the direction of Police's information strategy and roadmaps. The domain owners ensure that the Police Information Principles are applied in their domain and support development of the information roadmap for their domain.

Over the term of this strategy information governance will continue to promote positive, focused engagement between Police operational and corporate groups and the ICT Service Centre. With processes in place for monitoring and review (see Part 3), alignment between Police National Strategy and this strategy and the information and technology roadmaps will be maintained.

Data Lifecycle Management

Police will improve the management of data throughout its lifecycle. Our people-centric approach to information and systems will lead to simplified business processes, fewer information systems and less separately-managed data sources. This will lead to better data available for decision-making, and improvements in the quality of our statistical reporting.

Mobility devices have extended the point of capture to the field. We will progressively use context-based workflow to assist staff with data capture processes, automating and supporting capture where possible, and verifying data at the point of entry. This automated workflow will also help to control the flow of data into Police systems, since we already know that our ability to capture data outstrips our ability to process it.

We will move from many overlapping and interconnected data sources, each supporting its own vertical system, to two core data repositories that sit horizontally under our systems – one for core data required by Police operations, and one for documents and digital content that is not within core operational processes. These repositories will be authoritative for the many systems that store and link to data in them, such as our operational workflow, intelligence, planning and support systems. Police staff will have explicit and specific guidance on what information is authoritative (Master Data), where this information sits and the rules on how it is accessed. This will contribute to a strategic and planned approach to business and systems change.

Improvements in data quality – the technical correctness, timeliness, consistency and relevance of Police data – will be made through the use of data quality modelling, where quality issues and opportunities will be related to Business Consistency, Assurance or Partnerships. Business Consistency ensures a common understanding of data held in different areas, and will be improved through the progressive implementation of Master Data Management described above. Assurance deals with how compliant our data and data processes are with the Police National Recording Standard, which specifies what gets recorded and when. Partnerships with other agencies involve identifying data ownership and sharing that data according to agreed standards. The Police Data Quality Steering Group will oversee improvements to quality within the Police Records and Case Management System.

Information Sharing

Increasing levels of information sharing is a priority for Police as a natural result of the strategic focus on prevention. Increased expectation of integrated service delivery and improvements in offender pipeline processing (such as Electronic Courts) will drive the need for improvement in information sharing.

In particular, information sharing among Police and other Justice Sector agencies will be a critical element in achieving a more effective and efficient justice system, since information captured by Police informs Child Youth and Family (for young offenders), Courts, the Department of Corrections, and organisations such as Victim Support.

All information sharing that is undertaken by Police has to be in the context of the Privacy Act 1993, the Policing Act 2008 and other agency specific legislation. There is a natural tension between the need to improve outcomes (e.g. crime rates, service delivery, operational efficiency) and the boundaries on information sharing contained within legislation.

Information sharing is a complex area and it is necessary to consider the different forms of information sharing to enable the appropriate directions to be established. In the context of the ISSR we are limiting

the definition of information sharing to the sharing of information with other agencies within the New Zealand Public Sector, co-operating NGOs and other jurisdictions.

Police will work with the Department of Internal Affairs and our sector partners to drive the development and implementation of a common information sharing framework to improve the ability to share appropriate information efficiently.

INFORMATION SHARING CATEGORIES

The general categories of information sharing are as follows:

Knowledge Sharing: The provision of unstructured information related to the functioning of the agency, e.g. best practices, planning information, process and technical data, people capability, policy consultation etc.

Anonymised Data Sharing: The provision of structured data that is to be used with other data to provide insights without identifying specific people, e.g. official statistics, data for planning in the Justice Sector or local crime statistics.

Non-Anonymised Data Sharing: The provision of structured data that is to be used with other data to provide insights which identify specific people, e.g. to identify people at risk of harm, people that have propensity to cause crime or crashes, and general intelligence used in prevention.

Process Data Sharing: The provision of structured data that is used as part of a business process that extends across agency or entity boundaries and generally identifies specific people e.g. case (file) information provided to Courts, prisoner release information provided by Department of Corrections or information coming from the New Zealand Fire Service on events.

INFORMATION SHARING FRAMEWORKS

Increasingly, information is transferred electronically and in real time. In these circumstances standards, processes, and technology need to continuously improve to ensure that the information transferred is secure and legally compliant. For each information-sharing instance there needs to be in place:

Governance Definition: The process for providing oversight and decision making relating to the information sharing instance and ensuring clear accountability.

Agreement: The formalised definition of the arrangement including governance arrangements, context, allowable data usage (purpose), data transfer standards, data schemas, taxonomies and formats, operational arrangements and accountabilities.

Data Standards Definition: The standards describing how data should be structured for transfer between agencies and between countries (for example, Australia/New Zealand sharing of criminal histories). One data exchange standard with potential benefit for New Zealand Police and our partners is the National Information Exchange Model (NIEM) that was jointly developed by the US Department of Justice and the US Department of Homeland Security.

Technology Infrastructure Definition: The infrastructure that is used for the secure acquisition, storage, management and transfer of data – including agency information systems and networks.

Operational Process Definition: The processes that will either generate the data for transfer or receipt transferred data and process it in accordance with the purpose of the sharing arrangements.

Security Certification and Accreditation: The status of the complete set of information sharing arrangements (inclusive of governance, agreements, standards, infrastructure and operational processes) that ensure that the data is at low risk from loss or inappropriate access (such as a privacy breach).

INFORMATION SHARING HUB

There are increasing demands on Police for information sharing as other agencies establish processes for improvement of outcomes, such as those defined by Better Public Services. Police is increasingly becoming a “hub” for information as it sits within the Justice Sector (relating to the offender/victim flow), the Social Sector (relating to the protection of vulnerable people), Transport (improving road safety and reduction of crashes), Emergency Services (responding to major events) and increasingly in the Health

Sector (linked to mental health and alcohol related issues), Intelligence Sector (information related to national security) and others.

If these and future information sharing arrangements are to operate efficiently there needs to be standardisation around governance, agreements, data standards, technology infrastructure, operational processes and security arrangements. This aligns with the Government ICT Strategy and Action Plan which has activities relating to development of information hubs and other information sharing mechanisms designed to improve efficiency of information sharing arrangements.

Open Data

The Declaration on Open and Transparent Government was approved by Cabinet on 8 August 2011. In the declaration the government has committed to actively release high value public data. The intent is to enable the private and community sectors to use it to grow the economy, strengthen our social and cultural fabric, and sustain our environment. Through this commitment New Zealand citizens and businesses can expect a more efficient and accountable public sector, more services tailored to their needs, and a greater level of participation in shaping government decisions.

To support this declaration, the government asserts that the data and information it holds on behalf of the public must be open, trusted and authoritative, well managed, readily available, without charge where possible, and reusable, both legally and technically. Personal and classified data and information must be protected.

Police is an information-rich organisation. The data holdings we have are extensive and cover the complete range of Policing activities. This includes demand for services, data about people, vehicles and locations of interest and official crime and road policing related statistics. Police are required to release data under the declaration and must provide an ongoing plan for release to meet its aims.

The provisioning of raw data to the public will always be challenging for Police primarily because of the need to ensure privacy for individuals and to protect the core function of policing. Even raw data that does not provide details of people, but provides details of location can be combined with other data to indentify people – such as crime victims. However, it is recognised that this raw data has high value to people who are undertaking research or developing services in the crime prevention area. Therefore, we need to evolve the approach to data collection and dissemination and invest in tools in the business intelligence area that enable data to be provided in accordance with the declaration.

The Chief Information Officer is the delegated Open Data Champion responsible for ensuring that the intent of the declaration is fulfilled. PIMSEC is the oversight governance group on specific policy in this area.

Enabler 2: Information Security & Privacy

Evolving Information Security and Privacy Protection

The one global invariable is that information security and privacy is constantly evolving. Changing threat environments, technology innovation and the shifting focus means enterprise risks must be systematically assessed and effectively managed with minimal disruption to policing.

As a result of several high-profile information and privacy breaches Cabinet has mandated a series of directives calling for improved governance, better risk management performance and enhanced compliance from government agencies. Initiatives led by the Government Chief Information Officer (GCIO) and the Government Communications Security Bureau (GCSB) have focused on improving cyber security.

It is a fact of life that sensitive data traverses every enterprise network, that it is stored as many files types in various databases and must be readily available. Secure management of our information assets that encapsulates privacy and risk management underpins our drive towards operational improvements by ensuring information is available at the right time and to the right people. These aspirations bring with them significant challenges, including the risk of information loss, which are a result of:

- the rapid growth and dependency on technology
- an operationally distributed mobile environment
- outsourcing arrangements with partners, and
- an information explosion arising from new information channels (such as partner and public preference to engage with Police online).

Robust governance, supported by a methodical risk-based process, is needed to ensure that risks are appropriately mitigated. Information assets must have a known value, and be correctly classified based on their sensitivity and value to Police. Such an assessment of information assets will promote the design of effective information security and privacy protection policies that meet legislative requirements and address organisational priorities. In this way, the best use can be made of high-value data containing personally identifiable information or sensitive operational intelligence.

The overall focus for Police information security will be to ensure our critical information assets are adequately protected, that their value and classification is understood, that data loss safeguards are automatically enabled, and that it is clear where information is being created, modified, shared and stored.

The Information Security Framework

To put Police in the best position to meet Cabinet's directives a security framework has been implemented. The framework is the foundation underpinning security governance, information risk and assurance management for Police and is at the heart of all related security activities. PIMSEC provide domain owner governance over information. It oversees the processes, information and structure required to ensure the appropriate and adequate management of risk, including the accountability decisions on risk tolerance or treatment.

Information risk for Police is the practice of identification, assessment, treatment and measurement of threats and vulnerabilities to information assets. The process of selecting appropriate mitigations is based on risk, legislation, policy and standards. The core standards for Police are:

- The Protective Security Framework and Security In the Government Sector
- The New Zealand Information Security Manual
- The Privacy Act 1993
- The Police organisational approach to Risk Management , and
- The Police organisational security manual.

Our information assets are assessed to establish the current risk rating and identify an acceptable level of risk (the target state). This process involves the facilitation of workshops that can include technical and business representation. Mitigation strategies are developed which are based on controls that have been identified to comply with the core standards.

Controls will be selected based on their ability to reduce the impact and probability of a risk being realised. As an example, high probability, high impact risks will have mitigating controls selected from a library of controls to reduce both factors. Whereas, risks having a high probability but low impact will focus on mitigating controls that minimise the situation should the event occur.

Implemented controls are tested for appropriateness and assurance purposes. Outcomes are documented and an information asset certificate produced to show that the minimum level of compliance has been attained. This will be endorsed by the Police Information Technology Security Manager (ITSM).

For operational acceptance purposes, each information asset will be accredited and approved by the Police Chief Information Security Officer (CISO) to show the level of acceptable risk has been reached and that sufficient security measures are accepted.

Once an information asset has been accredited monitoring activities will be enforced to assist in assessing changes to its environment and operation and to determine the implications for the security risk profile and accreditation status of the system. Quality gates will be embedded into the system development life-cycle for this purpose and to ensure there is not a negligent impact on the approved risk status associated with the ongoing operation of the information asset. Operational security metrics will help to measure compliance with the core standards and policies.

Maturing capability

The organisation and management of Police information security is currently undergoing a fundamental restructuring so that the information security function can meet the increasing demands for enhanced security risk and privacy management. Independence over operational activities will be introduced. It will provide a separate governance and assurance function to assess metrics and management information to help demonstrate the correct operation of controls and measure compliance and effectiveness of information security policies.

Security and Privacy will be designed into our information assets and we will ensure there is an appropriate level of protection that is balanced with requirements for usability and availability. Improvements will be made in the way we protect our people, their identities roles and access to information. Information will be accurately classified, appropriately protected and made available to the right people at the right time irrespective of location or access point. Privacy impact assessment profiling will be used as a risk management tool to help maintain compliance with our privacy obligations.

We will introduce network-aware data loss prevention tools that monitor and provide near-real time alerts. We will detect inappropriate behaviours and report user and policy based compliance trends that present learning opportunities for the workforce. We will evolve a culture of security awareness, reduce the potential for data-loss and have the capability to effectively respond to and recover from security related incidents and crisis.

Our operational information assets and supporting infrastructure will benefit from increased governance, risk management and assurance oversight which will be delivered by ensuring systematic and ongoing assessment of changes to those assets. All future systems will be risk managed, operationally certified by the ITSM and accredited by the CISO.

Enabler 3: Design Thinking

We will integrate design thinking at Police to deliver information to our users in an Easy, Smart and Fast way. Design thinking will be embedded in all of our change initiatives.

Design thinking brings intuitive and rational thinking together from inspiration and ideation through to implementation. Inspiration is the problem or opportunity that motivates the search for solutions. Ideation is the process of generating, developing, and testing ideas. Implementation is the path that leads from the project stage into people's lives.

Design Thinking at Police will follow the five-stage Service Design lifecycle published by the Department of Internal Affairs in the R10 Service Design Toolbox (see Figure 7). This approach begins with understanding the intent and scope of business initiatives then follows an iterative, people-centric method of exploring and developing service concepts. The Service Design Specifications are used to assist developers in building and implementing a solution that delivers the agreed service. Finally the customer experience is evaluated post implementation and findings foster new understanding.

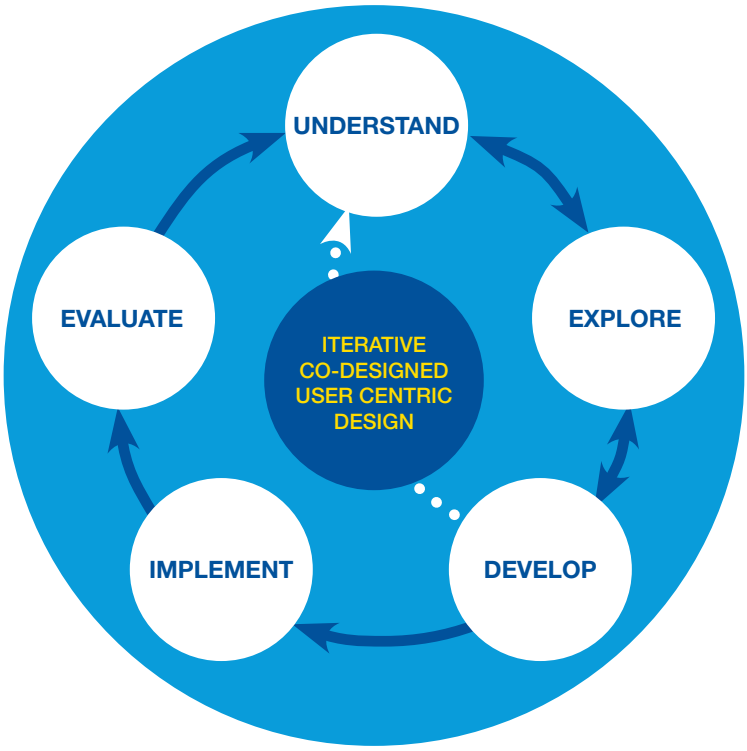


Figure 7: Service Design Lifecycle

Enabler 4: Technology Delivery

To deliver the information and systems required to meet strategy there are four areas of operation which we call the "Core Four" disciplines. They are Business Portfolio Management, Technology Management, Programme Management and Service Management. These disciplines ensure that consultation begins in advance of service design work and continues throughout the development lifecycle.

Business Portfolio Management

We use the Business Portfolio Management discipline to identify opportunities and channel ideas into ICT workflows, enabling business units and the wider emergency sector to deliver against their strategies by identifying where technology can enable outcomes. A close association with Programme Management helps to integrate new pieces of work into the delivery pipeline.

Business Portfolio Management develops a deep understanding of organisational and business strategies, and core business processes and drivers. It is the 'front door' for key stakeholders to access ICT services, and in this context it is used in managing relationships with Police executives, national managers and other agencies within the State Sector.

At Police, Business Portfolio Management will be organised across three key business areas: Innovation, Districts, and Inter-Agency Initiatives (including Emergency Response governance).

Technology Management

Effective systems lifecycle management smoothes the profile of technology investments and reduces technology risk and complexity. By taking advantage of technical innovation we will minimise the cost of support and upgrades, and remain compliant with our security obligations. We will also improve our ability to respond to organisational or legislative change, with increasing agility delivering fast and cost-effective change initiatives. This will result in reliable, stable information systems that deliver optimum levels of service continuity and resilience.

Police will maximise these benefits by putting in place clear asset management plans that key into our work programme. We will indicate our intentions, and communicate our infrastructure and application refresh plans appropriately. We will largely aim for an N-1 environment, so that we are up-to–date without assuming unnecessary technological risk. Where the benefits exist and the risks are understood and accepted, we will be prepared to operate on the latest versions of hardware and software.

We will use technology roadmaps to take advantage of opportunities to simplify our environment, such as major upgrades or end-of-life, removing complexity where possible through consolidation and rationalisation. The use of public cloud services will continue to increase in Police and we will take opportunities when they arise to reduce costs and improve services through this approach.

Police's own core ICT capabilities will be continually reshaped to reflect this approach to technology acquisition. We will rely more on partners to do things which are not core to Police, and we will share in common ICT capability across sectors and government as a whole. These initiatives will have a profound influence on the capability needs within the ICT Service Centre.

Programme and Project Management

Programme Management at Police provides the governance and frameworks needed to manage a portfolio of change initiatives that aligns with the ICT Delivery Plan, including project methodologies and risk management.

Programme Management at Police follows the PRINCE2 methodology, and is responsible for ensuring the delivery of the projects within programmes, and for the achievement and reporting of defined benefits. It works closely with Business Portfolio Management to understand upcoming ICT related initiatives and build a medium to long-term pipeline view. It also works closely with the Enterprise Project Management Office (ePMO) to ensure that its processes and reporting requirements are incorporated into ICT programmes, as well as the underlying projects.

Service Management

Police Service Management will optimise the delivery of information services to our users. We have positioned ourselves via the Police Service Hub to easily integrate Police and partner-provisioned services, to provide a single point of contact for assistance, and maintain service cohesion through a service heartbeat process. Using the Service Hub, we will develop an engagement model that partners can easily plug into, and that allows us to incorporate their capability and deliver it to our users quickly and seamlessly.

Using this approach to service management, key operational systems will be developed and modernised. The tools and technologies Police deploys will be fit for purpose, up-to-date and reliable, and will comply with current legislation. They will continue to meet the challenges we face, particularly our operational needs in the field, and provide the necessary resilience to save officers time and keep them safe.

Service Oriented Architecture and Enterprise Service Bus

To build the context-aware, intuitive experiences that our service design approach will identify with our users, we need to structure and develop our backend systems to allow for flexibility and agility. The approach we will take – Service Oriented Architecture (SOA) – breaks down the traditional system

silos into portfolios of more granular "services" (individual functions within systems that can be used and reused together as building blocks) to build business process-driven applications.

Our Enterprise Services Bus (ESB) sits above our backend systems and will be used to present the reusable building blocks to developers for rapid application development. At the same time, the ESB allows us to manage backend complexity by simplifying the interoperation of these systems, and avoids the duplication of connections and functionality.

The combination of the SOA approach to software development and use of the ESB will improve alignment between the business processes that we work with in service design and the systems that support those processes.

Enabler 5: Technology Partnerships

Police needs to continually acquire technology as new demands emerge and systems need replacing. This needs to be done in the context of information strategy and clear asset management plans. Police is moving from siloed system capability based on particular Police functions to systems that undertake generic functions shared by different Police processes. In this way we can achieve smooth flow of processes across the organisation, build underlying analytics and make systems easier for people to use. In such an environment we will require fewer systems, but potentially will encounter more complexity. So, we need to acquire technology differently. The general direction in this area is to develop long term partnerships, leverage all of government arrangements and focus internal resources on Police specific applications and integration.

Police is implementing partnerships with key suppliers across each of its core domains. The following long term partnerships are in place:

- **Mobility** – with Vodafone
- **Communications Centres** – with Intergraph
- **Data Centre** – with Revera
- **Enterprise Services** – with Gen-i

During the term of this ISSR, partnerships will be developed with suppliers for the following domains:

- **Fixed networks** – The core network connecting Police locations and systems
- **Land Mobile Radio** – The radio networks that provide wide area communication to Police officers for operational deployment
- **Application Development** – The development of our application software
- **Enterprise Resource Planning** – The provision of information to support decision making across all resources, money, people and assets.

We will continue to leverage all of government arrangements for technology supply and seek arrangements across the Justice, Emergency and Social Sectors that improve our ability to share information. Police has been a significant early adopter of GCIO-led ICT initiatives.

We will continue to take advantage of the purchasing power of government to reduce cost and procure improved services. In doing so, we expect to improve collaboration and information sharing through common technologies, and to deliver changes more quickly by leveraging pre-built solutions. Police will maintain an active role in shaping the direction of provision of ICT services across government, and in developing and managing our technology standards, we will aim to converge with cross government ICT standards.

Part 2: The Roadmap

Police Information Roadmap

Police Information Model and the Police Model

The Police Model has two key pillars built on a foundation of continuously improving support for the frontline: Prevention First and People and Victim Focus.

The model puts Prevention First because New Zealanders expect us to be in control of the criminal environment rather than simply reacting once things have gone wrong. The second pillar puts victims and witnesses, especially the vulnerable members of our society such as children, at the centre of our response, investigations and resolutions.

Together, the core elements of the two pillars – prevention, response, investigation, and resolution – provide a useful framework for considering operational policing:

Prevent: Prevention is at the forefront of everything we do, ultimately to reduce crime and crashes, gain greater control of the criminal environment and make New Zealand a safer place to live, work and visit. More focus on the underlying causes of offending and victimisation will ultimately lead to less crime and an improved service for victims.

Respond: Response begins when a call for service is received and recorded in police systems. We respond to calls for service, and at the initial attendance enquiries commence, evidence is gathered or other action is taken as necessary. Initial feedback is given to the victim. A detailed scene examination is conducted, forensic evidence is gathered and analysed and its relevance is assessed.

Investigate: After an initial assessment of the case, it is either closed (for lack of evidence or lines of enquiry) or referred to the appropriate group for investigation, and the victim is advised. A case that is to proceed is prioritised and assigned to an officer, and the victim is updated. An investigation is conducted to the point where a suspect can be identified and interviewed, and where all preliminary and follow up enquiries are complete. The victim is updated and frequency of ongoing contact is agreed.

Resolve: Resolution begins with a decision to prosecute or invoke alternate resolution (for example, pre-charge warning, Community Justice Panel). Where prosecution proceeds, agreed charges are entered into the Police records management system and submitted electronically to the Court. Court files are prepared and all pre-hearing actions completed. The victim's views on bail are sought and presented to the Court. After all hearings are completed the case is closed. Throughout this stage the victim continues to be updated.

This section sets out the future direction and priorities for information management at Police as they are aligned to prevention, response, investigations and resolutions, and also to the support areas engaged in continuous improvement for the frontline.

In the tables below, the priorities in each area of the Police Model are referenced with the predominant characteristic from the Police Information Model – Easy, Smart or Fast – to show a clear association between proposed action and strategic direction.

Prevent

Intelligence provides decision makers with the crime analysis and intelligence information they need to make decisions about timely and effective prevention.

Staff supporting investigations and operational staff in the field would like to be able to interrogate data and see patterns and relationships more easily and quickly. However, the critical work of identifying patterns of repeat victims, offenders and locations often needs to be redone when an updated intelligence report is required. Intelligence products, such as the scoring and ranking of crime triangle risk information (Victims, Offenders, Locations), which informs much of policing, can be continuously improved as Police gets access to up-to-date information across more internal and external data sources.

In the future, enhanced analytical capabilities will improve the breadth and depth of intelligence products such as entity extraction, predictive analytics, data mining, location mapping and data visualisations. Semantic sentiment analysis of social media will prove useful, for example, in anticipating emerging trouble spots. This and other forms of Big Data analysis will require us to cut through the information overload to extract relevant data. Moving away from email as the main sharing mechanism toward links to dynamic analyses will make it easier to share authoritative intelligence products internally, with partner agencies and with the public. More systematic management of the intelligence products' lifecycle will improve the review, approval and dissemination process, and lead to better traceability of decisions.

	PRIORITIES	2013	2018 TARGET
EASY	**IR-1** Increase use of social media to actively engage with the public	» Social media is used primarily at district level with a limited number of Police personnel being authorised to access social media sites. » Publicly available social media content is monitored as part of prevention.	» Police use social media as the major channel for community engagement and all officers use this as a primary engagement tool. » Police collaboration processes are based on the predominant and preferred social media services.
SMART	**IR-2** Increase automated analytical capabilities	» Intelligence information is compiled manually and disseminated.	» Trend analysis, modelling and risk scoring tools are used to identify emerging crime problems.
FAST	**IR-3** Distribute intelligence more effectively	» Intelligence products are shared mostly using secure email to groups or individuals on a need to know basis.	» Intelligence products can be viewed and manipulated, including interactive and dynamic mapping, in the field on any device with updates in real time. » Live intelligence is shared with other government agencies to present a common operating picture and improve crime prevention and response.
	IR-4 Improve information sharing between prevention agencies	» Information sharing to reduce crime, crash and victimisation occurs through "field co-ordination" and manual processes.	» Information is accessible (within defined access parameters) across partner agencies so that agencies can implement prevention interventions rapidly to reduce risk.
	IR-5 Increase access to information and data (as allowed by legislation)	» The ability to incorporate internal and external data sources into analysis is limited, and high levels of manual information transformation are needed.	» An information hub collects and aggregates source information for use in intelligence products, while protecting the integrity of the original data. » All relevant (and legally obtained) internal, external and public information sources are available for use in analysis.
	IR-6 Improve intelligence lifecycle management	» Manual version tracking of intelligence products reduces the usefulness of some reports.	» The lifecycle of intelligence products is a fully managed process supported by electronic workflow.
	IR-7 All road-side information capture is digital	» Approximately 65% of all Police infringements are issued electronically. This is limited by the availability of e-ticketing devices. » Analogue speed cameras are being replaced by digital cameras. » There is limited automated number plate recognition (ANPR).	» Accurate real-time vehicle and driver information, including heavy motor vehicles, road user charges and log book information can be captured and received electronically.

Respond

Communication centres receive emergency and 111 and non-emergency calls and coordinate and dispatch resources to attend events. Communications Centres will increasingly become contact hubs for the public, providing simplified access to Police services for people who prefer to call. The mode of interaction with communications centres is changing with the increased use of mobile devices. There will be extensive use of online and social media channels to engage with the public. Social media feeds will provide Police staff with access to richer information including photos and videos, around events.

The information available to communication centre staff for decision making is rapidly increasing with the improvement in analytics and the increased level of information coming in from the front line, other response agencies and the public. Deployment is about ensuring resources are made available at the right time and place to respond to events quickly and reduce crime and road trauma (tasking). There is increasing coordination at national, district and area level which requires accurate and timely Critical Command Information (CCI).

In the future, the availability of richer information will provide a real-time view of resource capability and its availability. There will be tools to track and analyse operational assets so they can be redeployed quickly and efficiently to where they are most needed. Better performance information will be available so officers can assess the effectiveness of operations and tactics as a key input for continuous improvements.

	PRIORITIES	2013	2018 TARGET
EASY	**IR-8** Ensure data only has to be entered once	» Data entry is manual with extensive use of paper forms, resulting in inefficiencies and variable data quality. » Information is not readily available for pre-populating forms, resulting in repetitive manual entry of basic information.	» Entering case information is easy as data entry screens and forms are intuitive and are dynamically populated. » Information standards are proactively monitored to identify and initiate resolution of any data quality issues.
EASY	**IR-9** Issue infringement notices in the field with fully automated processing	» Dedicated devices are used to issue infringement notices for road traffic offences.	» Infringement notices (for a wide range of offences) are able to be issued digitally from general mobility devices.
EASY	**IR-10** Introduce new modes of communication for the public	» The public requests emergency services by calling 111 through the telephone network and mobile phones. » Deaf, hearing impaired and speech impaired people can text if they are registered. » The Crime Reporting Line (CRL) processes non urgent requests for services by phone and email. » Community road watch reports are received by phone and online forms. » Police has a web and social media presence.	» The public can request services via a mobile application (Next Generation 111) and they are able to submit videos, images and engage via messaging and social media channels. » There is a single national number for non urgent calls to contact Police staff and make enquiries about cases. » There is an ability to report non urgent matters and get updates on progress of cases online and through mobile applications. » Important information can be proactively shared with citizens through a cohesive messaging and social media presence.
SMART	**IR-11** Provide front line officers with a common operating picture and information to support decision making	» Officers receive information in the field through mobile radio and mobility devices (calls, messaging and email). » Officers have information relating to response tasks on their mobile devices.	» Officers receive relevant, timely information and alerts on mobile devices and have a common operating picture with other officers, command and agencies.

	PRIORITIES	2013	2018 TARGET
SMART	**IR-12** Improve resource, location and deployment Information	» Officers provide status updates and locations either by mobility device or radio. » The radio dispatcher has visibility of officers within a geographical area and can allocate them to responsive tasks. » Analysis is undertaken to predict demand for more effective resource allocation based on time and location.	» At all times dispatchers have authoritative information on the location of officers, their competencies and their operational resources for optimal deployment to responsive, preventive and routine tasks. » Relevant information relating to events and tasks (such as intelligence products) is made available to communications centres, District Command Centres, officers and other response agencies in real time. » Predictive analysis dynamically adjusts resource allocation advice to commanders in real-time.
	IR-13 Improve Operational Resource and Asset Management	» Events and available resources (e.g. people, vehicle, tactical options) are aligned using primarily manual processes.	» There is an operational view of all resources and operational assets available for deployment at all times. » All operational assets, including vehicles, and tactical options are able to managed and allocated dynamically ahead of demand.
	IR-14 Improve Predictive and Simulation Capability	» There is some broad predictive analysis which shows the potential of crime and crash in geographical areas based on historical data.	» There is a high level of predictive information available to operational commanders at all levels with the ability to run simulations of events and undertake resource planning.
	IR-15 Create a Common Operating Picture	» Some event information is transferred between agencies (InterCAD) with co-ordination being primarily voice or location based (e.g. Fire and Police co-location). » Information sharing, with regular updates, exists for the different areas within the same Police.	» Communications Centres have immediate access to the most current information creating a common operating picture that can inform an integrated emergency services response. » Information is shared in real time, nationally across districts and with other response agencies providing a common operating picture.
FAST	**IR-16** Capture information in the field digitally and accurately	» There are a wide range of forms that require processing and manual entry. » Officers capture video, image and audio files and use email to transfer them to other systems using mobile devices. » Officers query Police systems for information about people, locations and vehicles using mobile devices. » Attendance applications (such as Family Violence) enable capture of essential information rather than fill out paper forms. » The Police National Recording Standard defines information requirements.	» All frontline workflow is managed through mobile devices and required information can be submitted in real time to Police systems. This includes the taking of fingerprints and statements, and the creation of case files and search warrant applications. » All information collected is validated at source and in accordance with standards, including attendance location where GPS can assist address identification.

Investigate

Police manages and resolves investigations using covert monitoring, electronic forensics, investigative interviewing, fingerprinting and other investigative tools and processes to provide better services for victims and promote safer communities. Today these services are mainly stand-alone and require manual interventions to manage the ingestion, securing and sharing of information.

In the future, investigation information will be supported by more automated processes leveraging core backend information systems. An integrated investigation platform that promotes national standards and processes will rationalise existing tools and information silos. Enhanced analytical capabilities, such as predictive analytics and entity extraction, will improve the breadth and depth of investigation services. Sharing information in the context of investigations will be easier.

	PRIORITIES	2013	2018 TARGET
SMART	**IR-17** Improve Information Capture and Review Processes	» Investigation information coming in is mostly paper based resulting in repetitive manual scanning of bulk documents.	» Investigation information is captured primarily in digital form and becomes accessible to investigations and intelligence systems. » Content analysis tools automate the process to find clues and identify leads within information held in digital media, allowing investigators to analyse relevant content rather than having to review all content.
	IR-18 Improve workflow support for investigations	» Investigation processes are documented in Police Instructions and files are developed using a combination of paper and electronic files.	» The investigation workflow is managed as an end to end process which is based on best practice and is continually improving.
FAST	**IR-19** Optimise use of digital media	» Investigative interviews use a standalone system, are stored on DVDs and are not readily accessible across Police. » Video and audio files captured in the field for investigations are retained in a standalone system.	» All digital media used in investigations is managed as part of an end to end workflow that can be used as evidence.
	IR-20 Simplify information sharing	» There are technical constraints on sharing large data files such as video and images. » There is limited sharing of fingerprint images between agencies. » Some critical information sharing processes are predominately paper based.	» All file formats and sizes are able to be transferred between systems without issue. » All essential information sharing processes between agencies and jurisdictions is based on electronic workflow that takes into account the legal constraints under which the information is provided, and automatically updates information as events and conditions change.

Resolve

Resolution occurs as part of the case management process and begins with the decision to prosecute or invoke alternate resolution. The Police Prosecution Service handles prosecutions in the District Court summary jurisdiction. The case management process records, manages and monitors reported offences from collection of the initial offence details through to case closure. This is a core operational process for Police and will continue to be the centre of information management. Efficiency will continue to be improved by automating major elements of data entry and improving management of case associated content such as documents images and video.

There will be increased focus on optimising workflow from the case management processes in Police and sharing of information regarding offenders and victims through the Courts to Corrections.

	PRIORITIES	2013	2018 TARGET
EASY	**IR-21** Create coherent digital evidence trail	» A nine step process is used to store documents relating to a case as attachments, in a repository with limited document/media management capability. » Images and videos taken in the field have to be manually attached to case files.	» All documents, images and videos relating to a case are linked to the case at the earliest stage in the process and a complete view of all material related to the case is easily accessible.
FAST	**IR-22** Enable appropriate sharing of case files	» Information is securely filed electronically in the Courts under the Justice Sector Electronic Operating Model (EOM). » Case disclosure information is filed electronically in court under the EOM with processes to ensure appropriate information is disclosed.	» Case files, with appropriate access protection, can be shared with Crown Solicitors and partner agencies.

Support Areas

Communication, Knowledge & Training

Effective internal communication with members is critical for the complex fast moving policing organisation. Collaboration, internally and externally is becoming increasingly important to manage the complex issues and relationships which are needed to support the reduction of crime and road trauma.

Police is increasing its training and development focus on operational outcomes while modernising delivery to the standards of other New Zealand tertiary providers. The main challenges are re-designing and implementing the initial training curriculum to increase focus on operational training, and moving away from paper-based training to digital-based training.

In the future, Police training delivery will be transformed into an anytime, anywhere activity through better access to online training materials and courses. We will build on the success of our initial training to embed operational, cultural and performance changes in the frontline.

	PRIORITIES	2013	2018 TARGET
EASY	**IR-23** Provide proactive relevant information to users through the best channel	» Information is provided through direct briefings, the Police Bulletin Board and email.	» The relevant Information is proactively provided to users in a manner, time and media they prefer with more use of digital content such as video.
EASY	**IR-24** Deliver Knowledge and Training Predominately On Line	» Most training, both initial and ongoing, is delivered at the Royal New Zealand Police College. Mandatory training delivered in districts is centrally managed. » Training materials and library resources are largely paper-based. eLearning courses are managed centrally within their own application.	» eLearning is designed specifically for mobility devices to foster anytime anywhere training. » There is a central place online to access learning material, including suggested courses based on previous learning, areas of development and skills shortages. » Sector wide library initiatives provide access to additional training and reference materials.
EASY	**IR-25** Increase the use of digital simulation	» A small number of simulations leverage technology to deliver training.	» Technology enabled training simulations can be shared across the Justice sector and with other relevant parties.
FAST	**IR-26** Implement collaboration tools that allow teams to share and work with information	» There is extensive use of tools such as Sharepoint and shared drives to provide information specific to workgroups and teams.	» A range of on line collaboration tools will be available for members to work together on cases, projects and initiatives and to share information.

People, Financial and Asset Resource Management

Finance processes ensure the financial resources of the organisation are used efficiently and effectively and the essential controls are in place as required by the Public Finance Act. Accurate and timely financial information is critical to Police managers at all levels to support decisions.

Human resource information is managed and safeguarded to ensure that it is reliable and accessible to employees and those responsible for deployment, operational and strategic decisions. It exists in a variety of formats, including paper, and in a number of systems.

Increasingly Police will move to enterprise resource planning (ERP), which will need to give an integrated real-time view of Police information and systems and the use of resources (financial, assets and people).

An integrated ERP will facilitate information flow between all business functions inside Police and manage external connections, such as Treasury and the Justice Sector.

	PRIORITIES	2013	2018 TARGET
EASY	**IR-27** Create a single authoritative source of finance and HR data	» Information exists within a number of systems in a variety of formats, including paper documents. » Physical personnel files are created and maintained for all Police personnel. A master file is held at Police Headquarters with a subset of content being held at the local station. Some personnel information, e.g. photos, is stored digitally. » Finance, HR and other data are in separate systems and require manual interventions to reconcile and get a total Police view.	» There is a single authoritative online (no paper) source of master financial and HR information that is accessible to systems and people requiring it to deliver business processes. » Information from paper-based personnel files has been digitised so it is searchable and useable by other systems and from any location. » Training records are digitised, reducing the need to retain physical examination papers and increasing accessibility to records by authorised personnel. » Recruitment wing information is consistently captured and is easily accessible to meet information requests and support recruitment decision making. » Training, skills and certification information is fully up to date and available to support deployment decisions.
	IR-28 Increase online self service for staff	» There is self service for the majority of HR processes but it is not intuitive and mobile.	» All core financial and HR processes are available on mobile devices and are role focused. » Members can develop their own reports, set alerts and review and approve financial management information wherever they are.
SMART	**IR-29** Improve financial and HR analysis	» The current financial data model supports basic analytical functions. Budgeting, forecasting and scenario modelling are inconsistent because there are a number of tools in use which use different assumptions and logic.	» Forecasting tools are much simpler to use, with capability focused on the development of driver-based models which are linked to performance targets.
	IR-30 Asset management	» Assets such as property and desktop computers have a good level of financial tracking, but financial tracking of operational, deployable assets is limited or lacking.	» Operational asset information is fully integrated into financial management processes, analysis and reporting.
FAST	**IR-31** Integrate planning processes using workflow	» Planning processes are primarily manual using data abstracted from systems.	» Scenarios can be developed for planning which are linked to core information and other plans. » Plans can be created, implemented and monitored with minimum manual intervention.
	IR-32 Automate and streamline HR and Finance Workflows	» Reliance on paper-based approval processes leads to inefficiencies, and a lack of electronic workflow makes it difficult to identify and remove processing delays.	» A near-paperless, workflow-driven, HR system maximises process efficiency and timeliness, accessibility of information, and self-service for staff, including those in the field using mobility devices. It also enhances the quality of information available to other systems and processes.

Governance, Policy and Performance Management

The Police Executive Committee, which is the governing body of New Zealand Police, is primarily a strategic forum focusing on the business cycle. It considers issues such as annual business planning and priorities, monitoring implementation of business plans and identifying 'big picture' risks to implementing them, key issues and initiatives, and operational issues with potential national implications. The Police Executive Meeting, a sub-committee of the Police Executive Committee, meets weekly to deal with the management of the organisation.

The Policy Group supports the Minister, the Commissioner and Police Executives by developing effective policies that reflect the Commissioner's strategic objectives and draw on the operational experience of Police, by providing a contact point for policy issues between operational Policing and internal and external stakeholders, and by providing and maintaining clear operational and administrative guidelines and instructions that everyone can access. Improved access to policy information via enterprise search and improved content management capability, along with a move away from manual processes to electronic workflow will provide better support for policy development.

Reporting has developed incrementally within specific areas of business need around operational applications, rather than more holistically in an efficient integrated Business Intelligence environment. In the future, we will provide authoritative data in a central location so that it can be used by everyone to make better decisions and improve reporting.

We will utilise advances in analytics to improve accuracy of statistical information, thereby reducing reliance on statistical expertise and reducing effort needed by analysts. We will also enhance the dissemination mechanism for performance information and reports to improve accessibility and timeliness, and to provide greater standardisation and flexibility.

Finally we will proactively embrace Open Data, increasing the frequency, quality and granularity of data published by Police. We will implement the tools and processes necessary to make greater use of increasingly available data in the public domain.

	PRIORITIES	2013	2018 TARGET
SMART	**IR-33** Make Performance information available to decision makers online and in real time	» Information from operational systems is reasonably accessible to those who request it. This can result in data being used in ways for which it was not intended leading to misinterpretation and inaccurate analysis. » A wide range of BI tools, applications and models exist throughout the organisation to meet specific analysis needs.	» Decision makers are easily able to directly access the performance information they need when they need it, without depending on analysts to produce routine reporting. » Decision makers have confidence that the numbers they see are robust, consistent with official figures, and able to be used and shared. » Redundant sources of information and associated BI tools, applications and models are decommissioned.
FAST	**IR-34** Make policy information more accessible and easier to manage	» Due to largely manual processes information from Police systems is not easily extracted and processed for research and policy development. » Managing source information and research analysis is difficult due to limited content management capability, including ready access to archived files.	» Digital workflow is introduced for all policy and cabinet papers. » Whole of enterprise search functionality enables users to search across Police information sources from a single user interface. » Police instructions are accessible from any device and links between content and to legislation are easily managed. Content is also accessible from within Police systems and applications.

Police Information Systems Development Roadmap

This section shows how Police systems will evolve over the next five years to meet strategic and operational needs. A Systems Inventory Map (See Appendix 1) describes the 2013 state of systems at a high level. A Police Future State Systems Model presents the 2018 state at a high level. In both cases "systems" may consist of a single application or a collection of applications which in combination provide a capability.

Current State

Until 2013 Police developed its systems in a siloed manner in response to the specific needs of Police operations. This has led to systems tightly coupled to Police operational functions with their own set of user interfaces, processes, data and infrastructure. Generally this has been supported by dedicated supplier arrangements. To enable processes to work end to end there has been significant customisation of systems to allow data to be shared. This has led to a very complex systems environment which is increasingly difficult to maintain and modify in support of new business requirements.

Principles for System Evolution

To evolve Police systems to the intended future state it is necessary to establish a series of System Evolution Principles which support decisions relating to areas such as the development or procurement of systems, design of business processes or location of authoritative data.

PRINCIPLE 1	Continuously seek to reduce the complexity of ICT delivery by standardising, consolidating and rationalising systems, data repositories and suppliers.
RATIONALE:	Reduces the number of discrete vertically integrated systems that have to be managed and therefore reduces the number of data, system and supplier interactions (and therefore cost and time) to develop and maintain services.
PRINCIPLE 2	Design new service experiences for people around intuitive interactions, embedded analytics and smooth flow.
RATIONALE:	Orchestrates various system components and data repositories to achieve a service experience for users that allows them to achieve their role in the most efficient manner – independent of the device they use and their location.
PRINCIPLE 3	Evolve applications to be components that deliver specialised information and workflow services needed to support Principle 2.
RATIONALE:	Uses a service oriented architecture approach to break vertically integrated applications down to their components that can interact with other systems and data repositories in a flexible way, present to end users as context-aware business processes or functions that can be reused, and be continuously improved and adapted to meet new requirements. The resultant user applications will mirror the real-world activities of our users. This extends to using components provided by other agencies and external providers.
PRINCIPLE 4	Evolve to a Police Core Information Repository that is a logical repository for all operational information.
RATIONALE:	Brings together logically data about people (including biometrics), vehicles, locations, businesses, events and Police resources into a data architecture which defines authoritative data that can be accessed by applications for the purpose of providing services.

Police Future State Systems Model

Applying the System Evolution Principles to the current systems inventory enables a Police Future State Systems Model to be developed. The model provides a conceptual view of the minimum level of systems required to deliver the services to users, and will be a reference point when determining end states and transition states for systems.

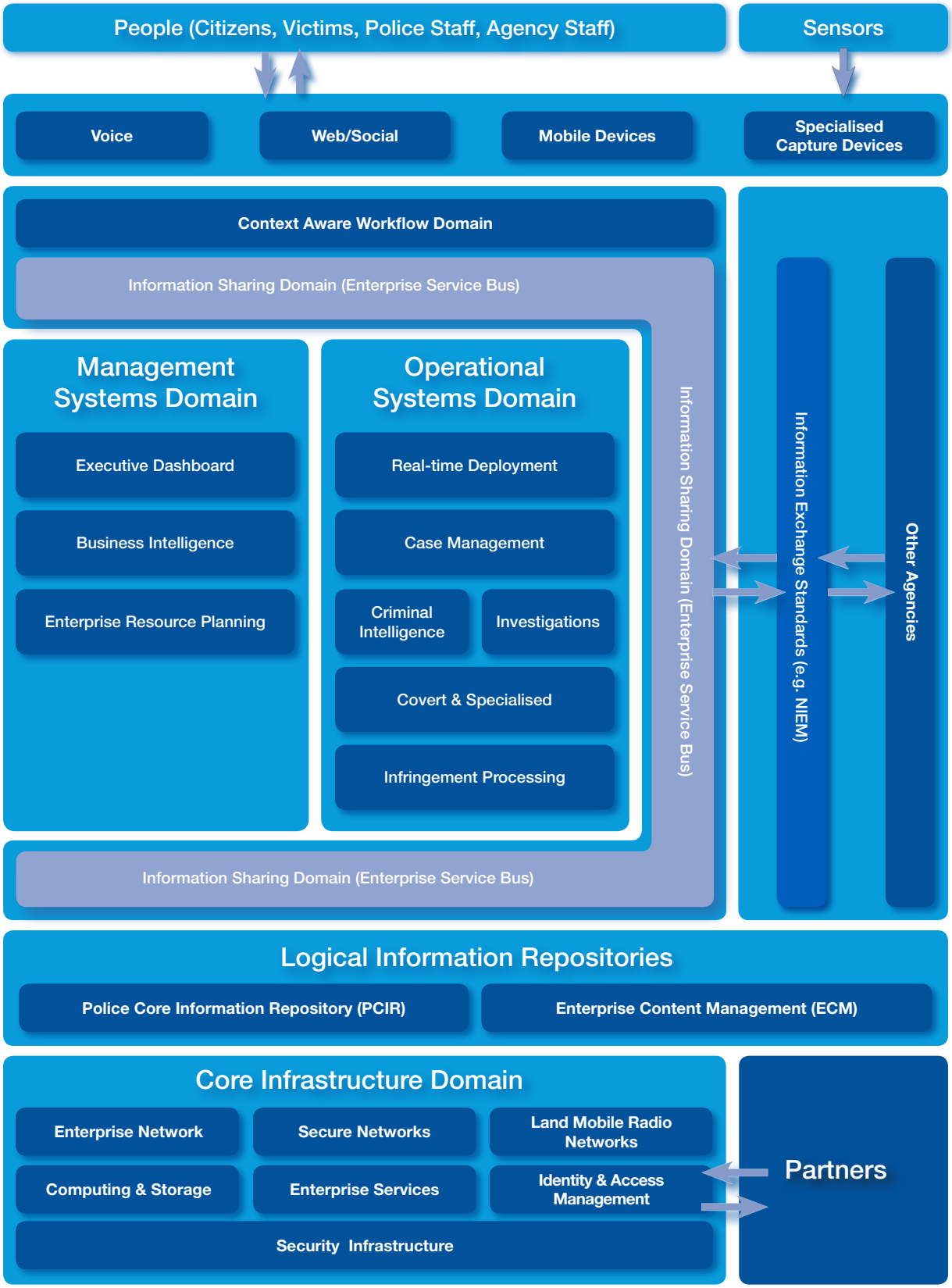


Figure 8: Police Future State Systems Model

The direction for systems development that meets the needs expressed through the roadmaps is set out below. Expected timeframes for development are:

[S] By the end of 2014

[M] By the end of 2016

[L] Beyond 2016

DIRECTION	SYSTEM DOMAIN	IMPLICATIONS
DIGITAL ACCESS		
SD-1 Enhance the public's ability to communicate with Police through voice channels by rationalising voice platforms and aligning service delivery more closely to non-voice channels	Voice	SD -1/1 Consolidate all voice platforms (e.g. communications centres, unified communications, station based services) to enable streamlining of call flows (integrated contact) to and from Police operational units, and support alignment with non-voice channels. **[S]** SD -1/2 Implement technologies such as biometrics and voice recognition to increase efficiency, improve caller response and achieve early call resolution. **[M]** (Aligned to Result 10)
SD-2 Enable the public to access Police information and services and transact on line	Web /Social	SD-2/1 Develop capability to establish and manage a presence on the (mobile) web and through Smartphone applications so that information can be provided to the public, and the public can provide information and undertake commonly used transactions. **[S]** (Aligned to Result 10)
SD-3 Increase Police staff access to services through any appropriate device (PC, tablet, phone, website) at any location	Mobile	SD-3/1 Evolve services and platforms – through mobility, workflow management and identity and access management – to present services on any appropriate device and anywhere. **[S]**
SD-4 Increase capture of information from specialised devices such as automated Sensors (e.g. speed cameras), and devices used by people (e.g. Tasers and other image/ data capture devices). Note: this is subject to legislation	Specialised Capture Devices	SD-4/1 Evolve the capability to manage the information coming in from an increasing range of digital acquisition devices. **[M]**
CONTEXT AWARE WORKFLOW DOMAIN		
SD-5 Implement service orchestration for all users (internal and external) that integrates application level processes and ensures a smooth (work)flow	Context Aware Workflow	SD-5/1 Develop a common Workflow Management Platform (WMP) architecture and acquire new technology if required. **[S]** SD-5/2 Evolve eQUIP to provide workflow for the Front Line and align to the choices made for WMP. **[S]** SD-5/3 Consolidate the workflow from systems such as NIA, S&S and CRIS into the WMP. **[M]** SD-5/4 Develop WMP to support on-line services delivered to the public. [M] Refer to SD-2/1.
INFORMATION SHARING DOMAIN		
SD-6 Implement a Service Oriented Architecture(SOA) approach to development to simply and speed up application development	Enterprise Service Bus	SD-6/1 Extend the Enterprise Service Bus (ESB) to expose reusable interfaces (web services) to applications, for both user-application and application-application information interactions (to users and external agencies). **[M]**
SD-7 Provide standard data exchange interfaces into information repositories and processing systems for other agencies systems	Information Exchange Standards	SD -7/1 Develop a standard data exchange (information sharing) model and capability (AoG or Sector Level) using standards (such as NIEM), and made available via the ESB. **[S]**

DIRECTION	SYSTEM DOMAIN	IMPLICATIONS
MANAGEMENT SYSTEMS DOMAIN		
SD-8 Improve Executive visibility of the end to end performance of Police in real time	Executive Dashboard	SD-8/1 Develop information analysis and dashboard presentation capability. **[S]**
SD-9 Improve access and analysis of core Police information and other sources to provide insights for Business Intelligence	Business Intelligence	SD-9/1 Develop the data architecture and supporting database technology to enable simplified and standardised access to data. **[S]** SD-9/2 Rationalise Business Intelligence (BI) systems (including SAS and BO) to create a single BI platform. **[M]**
SD-10 Evolve to an integrated system that provides information to supports performance and decision making across all Police resources, money, people and assets	Enterprise Resource Planning (ERP)	SD-10/1 Expose data in ERP applications (PS and SAP) to support services such as Executive Dashboard, BI and Real-time Command & Control. **[S]** Refer to SD-9. SD-10/2 Consolidate HR, Finance and Workforce Management Systems into one Enterprise Resource Planning (ERP) system platform. **[L]**
OPERATIONAL SYSTEMS DOMAIN		
SD-11 Enhance real time command visibility (Common Operating Picture) of Critical Command Information for deployment relating to prevention and response activities	Real-time Deployment	SD-11/1 Continue to expand RIOD capability relating to aggregation and presentation services for real time command and control information. **[S]** SD-11/2 Rationalise geospatial platforms and servers to improve information access and command visibility of events and resources. **[S]** Refer to SD-9.
SD-12 Increase workflow support for cases from collection of the initial offence/event details through to case resolution and interfacing to Courts	Case Management	SD -12/1 Improve workflow capability to manage digital evidence. **[S]** Refer to SD-7 and SD-17. SD-12 /2 Separate case management workflow from the NIA system core and include in workflow management platform. **[M]** SD-12/3 Rationalise CARD and NIA capability to a unified information architecture to smooth the workflow end-to-end. **[L]**
SD-13 Improve access and analysis of core Police information and other sources to provide insights for Criminal Intelligence and management of "persons of interest"	Criminal Intelligence (including "persons of interest")	SD-13/1 Create advanced search capability across all Police data linked to data access rights. **[S]** SD-13/2 Develop existing systems (e.g. Investigator, NIA) to deliver criminal intelligence and "persons of interest" management. **[M]**
SD-14 Increase automation of processes of complex and covert investigations	Investigations	SD -14/1 Increase the range of investigations types in the investigations workflow system. **[M]** SD -14/2 Integrate Investigator with Criminal Intelligence, PCIR and Case Management to ensure coherent workflow and data management. **[M]**
SD-15 Improve acquisition and analysis of digital data and evidence required for complex and/or or covert investigations	Covert and Specialised	SD-15/1 Align and evolve systems used for the management of digital evidence and investigations. **[M]**
SD-16 Improve infringement processing (traffic, alcohol and others) from the point of notice issue until payment	Infringement Processing	SD -16/1 Evolve the infringement processing system (PIP) to improve workflow. **[S]**

DIRECTION	SYSTEM DOMAIN	IMPLICATIONS
LOGICAL INFORMATION REPOSITORIES		
SD-17 Create a logical repository for all core Police data required for operations	Police Core Information Repository (PCIR)	SD -17/1 Implement information classification to support data access management. **[S]** SD -17/2 Develop identity and access management to provide access control (security) over core data. **[S]** SD-17/3 Logically separate the data repositories from NIA and CARD to provide the basis of the PCIR. **[S]** SD-17/4 Develop data access interfaces from PCIR to client systems such as CCI (RIOD), Business Intelligence and Criminal Intelligence. **[M]** SD-17/5 Enhance AFIS to include wider range of biometric information and align as part of the logical structure of PCIR. **[M]**
SD-18 Create a logical repository for documents and digital content that is not within core operational processes	Enterprise Content Management (ECM)	SD-18/1 Acquire capability for integrated digital content management and migrate non-operational data to this repository. **[M]**
CORE INFRASTRUCTURE DOMAIN		
SD-19 Consolidate and rationalise the core network connecting Police locations and systems at a RESTRICTED level	Enterprise Network	SD-19/1 Develop a network architecture for ensuring bandwidth needs availability and resilience. **[S]** SD-19/2 Rationalise the network technically, operationally and commercially. **[S]** SD-19/3 Increase level of network monitoring capability at the border to reduce security risks. **[S]**
SD-20 Continue to develop the network connecting Police locations and other agencies at a TOP SECRET LEVEL	Secure Networks	SD-20/1 Evolve the secure networks in accordance with requirements from partner agencies. **[S]**
SD-21 Continue to evolve land radio networks that provide wide area communication to Police Officers for operational deployment	Land Mobile Radio Networks	SD-21/1 Evolve networks to provide broadband wireless capability and support dedicated emergency services requirements as per the Whole of Government Radio Network (WGRN). **[M]**
SD-22 Increase use of logical infrastructure that provides the processing and data storage capacity for systems	Computing & Storage	SD-22/1 Evolve Infrastructure as a Service (IaaS) to become Platform as a Service (PaaS) and remove Police's need to manage hardware (private cloud). **[M]**
SD-23 Provide up to date general office productivity services, including email, information storage and retrieval and word/document processing	Enterprise Services	SD-23/1 Develop the Enterprise Services Platform (ESP) to increase the range of services and improve usability. **[S]**
SD-24 Provide the ability for users to access services and applications in accordance with their role	Identity and Access Management	SD -24/1 Acquire role based Identity and Access Management (IAM) for all Police systems to support effective workflow management and information security. **[S]** SD -24/2 Implement RealMe for all public facing access management. **[M]**
SD-25 Improve the implementation of security policies, including firewalls, certificate authorities and monitoring	Security Infrastructure	SD-25/1 Consolidate the management of the security domain. **[S]** SD-25/2 Acquire and enhance security monitoring capability. **[M]**

Part 3: Delivery and Alignment

Police ICT Delivery Plan

The Police Information and Systems Strategy and Roadmap will be implemented via the Police ICT Delivery Plan, which is reviewed quarterly by the Police Executive.

ISSR Alignment, Monitoring and Review

The success of the Police Information and Systems Strategy and Roadmap will be determined by the extent to which the outcomes it achieves contribute to delivery of the overall police objectives of reducing crime and road trauma and of increasing public trust and confidence in Police.

It is clear that there are inextricable links between Police's broader strategy and this information and technology strategy. Therefore this document must be seen as a piece of the overall strategy and reviewed when the Police's strategy adapts and changes over the next five years. This ISSR also must be implemented, so there is a clear connection with the allocation of people and financial resources by the Police Executive.

This ISSR will be aligned, monitored and reviewed at a number of levels and timeframes. There will also be different mechanisms for implementation depending on the specific type of direction. These are summarised below.

ASPECT	GOVERNANCE ENTITY – PROCESS	FREQUENCY
Alignment to Police Strategy	Police Executive	Annually
Alignment to Government ICT Strategy and Action Plan	CIO on behalf of Police Executive with GCIO	As required by GCIO
Alignment with resources (people and priorities)	Police Executive by approval of the ICT Delivery Plan	Quarterly
ICT Investment alignment with the plan	Business Cases must demonstrate alignment to the ISSR and be considered by PIMSEC	As required
Information-related standards, policies and processes	New policy and processes must demonstrate alignment to the ISSR and be considered by PIMSEC	As required
Technology Standards and Architectures	Changes to technology standards and architectures must demonstrate alignment to the ISSR and be considered by the Technical Advisory Group (TAG)	As required
Acquisition of new technology capability	New systems must demonstrate alignment to the ISSR through each phase of procurement	As required
Monitoring Implementation of the ISSR and ICT Delivery Plan	Police Executive	Quarterly
Monitoring of programme and project management capability	Police Enterprise Portfolio Management Office	Monthly
Monitoring of the information security implementation	Chief Information Security Officer	Monthly
Monitoring of the implementation of Enablers	CIO supported by the ICTSC Senior Leadership Team	Monthly

Appendix 1 – Police Key Systems Inventory 2013

The following diagram shows the Police Systems Inventory in 2013. It is a significantly simplified view of Police systems to support the description of the Systems Roadmap. A description of the systems within the inventory is set out below.

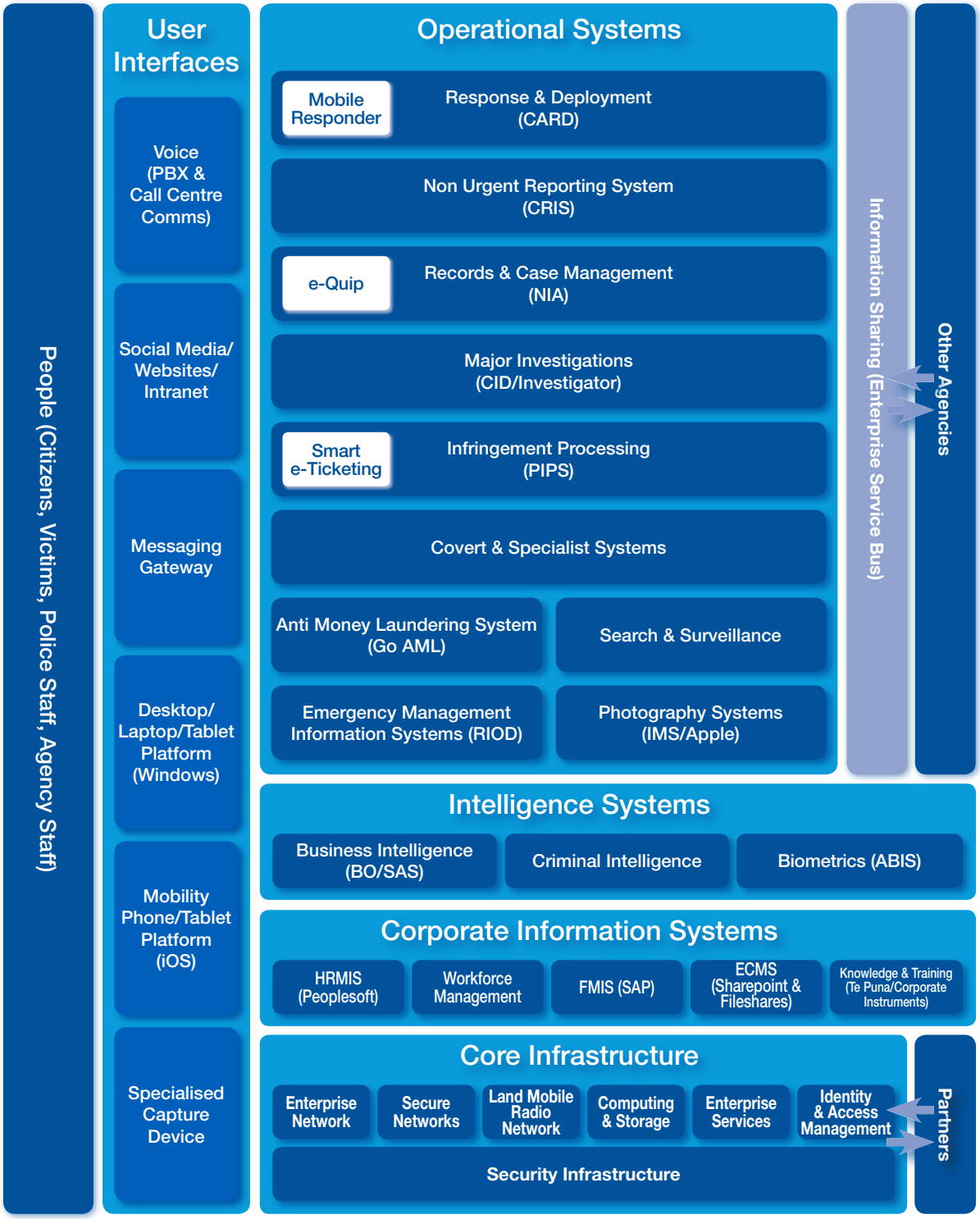


Figure 9: Police Key Systems Inventory 2013

The following table provides an overview of the systems in use in Police in 2013 and their key functions.

FUNCTION	SYSTEM	DESCRIPTION
OPERATIONAL SYSTEMS		
Response and Deployment	CARD (Intergraph)	Workflow support and data repository for managing the deployment of resources in real time. Included is mobile workflow support for Police Officers (Mobile Responder)
Non-urgent Crime Reporting	CRIS (Police)	Workflow support for capture of historical and non-urgent crime
Records Management	NIA (Police)	Retention and management of records for offences, locations, people and vehicles
Case Management	NIA (Police)	Workflow support for cases from collection of the initial offence details through to case closure and interfacing to Courts
Mobility Interface	eQUIP (Police) Mobile Responder (Intergraph)	Workflow support for front line Police Officers for undertaking routine duties
Investigations	CID(under replacement) Investigator (Wynyard)	Workflow support and data repository for complex investigations
Infringement Processing	PIPS (HP)	Workflow support and data repository for traffic and alcohol infringement processing
Anti-money Laundering	GoAML (UN)	Workflow support and data repository for the identification of money laundering transactions
Covert and Specialised Forensics	Various	Workflow and analysis for covert investigations, legal interceptions and digital forensics
Search and Surveillance	S&S (Adobe)	Workflow support for the processing of warrants, including search warrants and surveillance device warrants
Emergency Management Information Systems	RIOD (Platform)	Workflow support for special events and command and control at national and district level
Forensic Photography	Various	Workflow support and data repository for the processing of images and video for evidence purposes
INTELLIGENCE SYSTEMS		
Business Intelligence	Business Objects and SAS	Analytical support for legislative reporting, formal statistical purposes, performance management and decision support
Criminal Intelligence	From 2014	Analytical support for enhanced intelligence for prevention of crime
Biometrics	AFIS (NEC) and Image Management System	Workflow support, matching analytics and data and image repository for finger and palm prints and prisoner and firearms licence photos
CORPORATE SYSTEMS		
Human Resources	HRMIS (Oracle)	Workflow support and data repository for time recording, payroll, training records, position management and performance management
Workforce Management	Aspect (Calldesign)	Workflow support for the management of human resources and allocation to work duties
Financial Management	FMIS (SAP)	Workflow support and data repository for financial management processes and information

FUNCTION	SYSTEM	DESCRIPTION
Electronic Content Management System (ECMS)	Sharepoint & File shares	Workflow support and data repository for the creation and tracking of documents and multimedia material on the network that do not exist within core operational systems
Knowledge Management	Various	Information repositories for on-line training, Police Instructions and general information
CORE INFRASTRUCTURE		
Enterprise Networks	Various WAN Suppliers	The core network connecting Police locations and systems at a RESTRICTED level including fibre, microwave and data services and the management systems
Secure Networks	Various WAN Suppliers	The network connects Police locations and other agencies at a TOP SECRET LEVEL
Land Mobile Radio Networks	Digital (Tait P25) Analogue (Various)	Radio networks that provide wide area communication to Police Officers for operational deployment
Computing and Storage	Data Centres (Revera) Equipment (Various)	Physical infrastructure that provides the processing and data storage capacity for systems
Enterprise Services	Various (primarily Microsoft)	Provision of general office productivity services, including: email, information storage and retrieval and word/document processing
Identity and Access Management Systems	Various (primarily Microsoft AD)	Provides the ability for users to access services and applications in accordance with their role
Security Infrastructure	Various	Supports the implementation of security policies, including; firewalls, certificate authorities and monitoring
ELECTRONIC INFORMATION SHARING INTERFACES		
Data Exchange	Various	Support the flow of information to and from other agencies, which are primarily specific to a system
ELECTRONIC USER INTERFACES		
Voice Services	Cisco PBX Solidus Call Distribution	Provides voice connection capability between Police staff and the public and Police Staff. Includes complex call routing for communications centres and general administrative calling
Web Site, Social Media	Various	Provides the public with information through internally provided websites and general social media channels
Intranet	Various	Provides Police staff with information and access to systems
Messaging Gateways	Various	Provides access to and from the public via SMS and MMS
Laptop/Desktop/Tablet	Various (Windows)	Provides Police staff with the ability to access systems and information through various devices (9000+ devices in use)
Mobility Phone/Tablet Platform	Various (mainly Apple iOS)	Provides Police staff with remote access to systems and information (10,000 devices in use)
Specialised Capture Devices	Various	Provides capture of information from specialised devices such as speed cameras, Tasers and other image/data capture devices

Appendix 2 – Alignment to Government ICT Priorities

Government ICT Strategy and Action Plan

This ISSR aligns with the Government ICT Strategy and Action Plan to 2017, taking due cognisance of the Strategy's objectives, guiding principles and four focus areas. Aspects of this ISSR demonstrating alignment with the four focus areas, including system assurance activities in each area, are listed in this Appendix.

Services are digital by default

- Police strategic direction – Place people at the centre (p7)
- Intuitive interaction – Making it easy (p9)
  - FC1 – Social Media
  - FC2 – Identity Awareness
  - FC3 – The Digital Channel
  - FC4 – Applications
  - FC5 – Mobility
- Smooth flow – Making it fast and efficient (p13)
  - FC12 – Case management
  - FC15 – Citizen engagement
- Design thinking (p22)
- Technology delivery – Service management (p23)

Information is managed as an asset

- Information Management – Information Principles (p15), Information Governance (p16), Open Data (p19)
- Information Security & Privacy (p20)
- Part 3 Delivery and Alignment (p39)

Investment and capability are shared

- Police Future State Systems Model – Context Aware Workflow Domain (p36), Information Sharing Domain (p36), Operational Systems Domain (p37), Logical Information Repositories (p38), Core Infrastructure Domain (p38)

Leadership and culture deliver change

- Technology Delivery (p22)
- Technology Partnerships (p24)
- Police Information Roadmap – Police Information Model and the Police Model (p25)
- Principles for System Evolution (p34)

Better Public Services – Result 10

New Zealand Police is one of eight key agencies helping to shape the direction of digital service initiatives so that people will increasingly use the digital channel for their transactions with government. In particular, the strategic direction, capabilities, enablers and priorities listed below provide alignment with Result 10, and will ensure a strong Police contribution to the above target.

- Police strategic direction – Place people at the centre (p7)
- Intuitive interaction – Making it easy (p9)
  - FC1 – Social Media
  - FC2 – Identity Awareness
  - FC3 – The Digital Channel
  - FC4 – Applications
  - FC5 – Mobility
- Smooth flow – Making it fast and efficient (p13)
  - FC12 – Case management
  - FC15 – Citizen engagement
- Information management – Open Data (p19)
- Design thinking (p22)
- Technology delivery – Service management (p23)
- Police Information Roadmap – Priorities (p25)
  - Prevent – IR1 Increase use of social media to actively engage with the public
  - Respond – IR9 Issue infringement notices in the field with fully automated processing

www.police.govt.nz