



Information, Communications and Technology Strategic Plan

2005 – 2010

Table of Contents

- From the Minister 1*
- From the Deputy Commissioner..... 2*
- 1. ICT Strategic Plan Outcomes..... 2**
- 2. Key Relationships..... 2**
- 3. Principles..... 3**
- 4. Governance..... 3**
- 5. ICT Strategy 4**
- 6. User Strategic Themes 9**
- 7. ICT Strategic Technology Themes 9**
- 8. New Initiatives..... 10**
- 9. Workplan..... 11**
- Appendix 1 ICT Strategic Plan Review and Update Process 13**
- Appendix 2 Progress Since Last ISSP 15**
- Appendix 3 The Ongoing ICT Enterprise Refresh..... 16**
- Appendix 4 Business Initiatives..... 16**
- Appendix 5 Prioritised Business Initiatives by User Theme..... 17**

From the Minister

As Minister of Police I am privileged to provide support to Police's Information, Communication and Technology (ICT) Strategic Plan for 2005-2010.

I know the successes that Police has delivered over the last few years, in terms of crime and crash reduction and record clearance rates, are due in no small part to its' information, communications and technology tools.

I support the Commissioner on providing Police with a world class technology platform to enable Police to meet the challenges that the next five years will present. The ICT systems upgrade began with the successful migration from the Law Enforcement System to the National Intelligence Application. With this Police introduced an ICT platform that will enable services to be delivered to the community more effectively than ever before.

One of the most pleasing aspects of this plan is that the new initiatives are being driven by frontline staff. I commend Police and the ITSC staff for this approach and believe the solutions will be robust and enduring as a result of this front end buy-in.

I look forward to seeing the work programmes and deliverables outlined in this plan coming to life.



Hon Annette King
Minister of Police



From the Deputy Commissioner

I am pleased to present the New Zealand Police Information, Communications and Technology (ICT) Strategic Plan for 2005–2010.

The plan recognises the importance of ensuring that we all have the most appropriate ICT tools to do our jobs professionally. It aims to provide mobility at the frontline, increase the speed of police work, and reduce paperwork wherever possible.

Specifically the plan aims to provide tools to:

- improve service to the community
- improve intelligence and investigative capability
- maintain security and integrity of information
- improve deployment
- reduce repetitive paperwork; and
- improve reporting.

Building on the solid infrastructure put in place over the last five years, the ICT Strategic Plan 2005-2010 provides the framework for both the stability needed for us to undertake our day-to-day work, and the further development required for our systems to keep pace with the changing demands of modern policing.

To this end, the strategic plan confirms a continuing and substantial programme of ICT infrastructure refreshment, upgrade and uptake of new options.

It also defines a significant series of new initiatives, prioritised by frontline staff, to enable policing services to be delivered to the community.

I'd like to thank the ICT staff for their hard work and their commitment to supporting frontline and administrative operations and, in particular, thanks to all police members involved in the development of this strategic plan.

I commend the plan to you and encourage you to work together to turn these words into action.



Lyn Provost
Deputy Commissioner



1. ICT Strategic Plan Outcomes

Police Strategic Plan Safer Communities Together outcomes:

- Reduce violence
- Reduce burglary
- Reduce vehicle crime
- Reduce organised crime
- Increase national security
- Enhance road safety

Police Organisational Development Focus for 2005/06:

- Capability
- Service management
- Integrity

Mandate

- NZ Police ICT standards will be adhered to for all ICT related design, build, purchase, maintenance and replacement
- New initiatives will be subject to the budget process and approved business cases
- All ICT-related purchases, implementations and systems maintenance will be managed by ITSC.

2. Key Relationships

New Zealand Government Agencies

Government initiatives for more electronic government service delivery will continue to guide Police ICT direction.

Exchange of information between agencies will increase. Under applicable legislation Police expects to provide secure access for these agencies to relevant Police systems and information, and vice versa.

The Information, Communications and Technology (ICT) Strategic Plan supports the community safety, and crime and crash reduction outcomes in the Police Strategic Plan and annual Statements of Intent.

It provides the framework for aligning information, communications and technology implementation and support priorities, with Police's strategic outcomes and medium term organisational development focus.

It defines ICT direction, standards and governance within Police and provides the framework for ICT development and operations for 2005 – 2010.

These developments and operations will be delivered through a combination of ICT "Business as Usual" and "New Initiatives".

Business as Usual activities will ensure the availability, security, integrity, capacity and currency of the ICT systems, in combination with a programme of improved ICT service delivery.

New Initiatives will provide additional capability to Police ICT systems, addressing organisational development themes of:

- Capability, through improving intelligence, investigations and deployment
- Service management, through improving service access, reducing repetitive paperwork and improving integrated reporting, and
- Organisation performance, through maintaining the security and integrity of information.

The initiatives are targeted at enabling improvement in the effectiveness and efficiency of core policing functions. Critical success factors include:

- Ease of access to ICT systems
- Ease of entering, updating and retrieving information
- Smarter processing of information, to increase knowledge
- Improved information through ICT systems interfacing and integration, and
- Risk mitigation.

The Community

Police will continue work on improving the service provided to the public through protecting public safety and reducing crime and crashes. Police will also work on initiatives to enhance the effectiveness of both emergency and non-emergency communication between the Police and the community.

The Police website will continue to develop both general and targeted information, in collaboration with public stakeholders, to assist crime prevention and public safety awareness.

Justice Sector and Government Initiatives

Police will maintain interfaces with other central government, local government and supporting agencies, including:

- Justice sector
- Emergency management sector
- Road safety, and
- Other key agencies in areas such as border and bio-security, land management, social agencies, and local government.

3. Principles

Technology Trends

In preparing the ICT Strategic Plan Police have recognised the following technology trends:

- Capacity will increase and unit costs will decrease
- Mobile access will mature and uptake will increase
- Information management moves to knowledge management
- Information will become more secure
- Integration and interface technologies will bring together disparate systems
- Usability will improve
- Presentation of information via multimedia will increase
- The use of electronic surveillance will increase
- Uptake of commercial off-the-shelf applications will increase
- Convergence and integration of video, audio and data.

Guiding Principles

The guiding principles for the ICT Strategic Plan are:

- strict alignment between the Police Strategic Plan and the ICT Strategic Plan
- continuing a programme of strategic partnering
- ICT capability development will be incremental and evolutionary
- a programme of long-term progressive investment, to build and maintain the ICT environment
- ongoing initiatives and projects maintaining the currency of the ICT environment
- ICT projects will be properly managed, with sound governance
- “ICT Guardianship”, protecting and nurturing the investment in ICT resources
- adherence with Government directives
- all Police ICT projects will comply with Police ICT standards and specifications, based on open system technology
- the increasing use of commercial off-the-shelf applications customized for Police, while recognizing that some specialist applications may need to be built in-house, and
- all Police ICT purchases must be through ITSC.

Police recognise that both the Police environment and the ICT environment are dynamic and changes will occur. Therefore the ICT work programme will be reviewed annually to determine if new initiatives are necessary and to reprioritise all initiatives.

4. Governance

The ICT Strategic Plan requires explicit support through:

- ongoing commitment to the guiding principles and resulting workplan from the Police Executive
- sound financial management that fully identifies and manages the technology and business costs, and
- sound and disciplined project management with clearly defined roles between the business and the ITSC.

ICT Advisory Board (ICTAB)

ICTAB’s role is to monitor major ICT initiatives from a business context, including their interrelationships with other projects. ICTAB is comprised of a group of senior Police executives, supplemented by external experts.

Financial Management

Formal policies are in place, providing the mandate and processes for financial management, including budgetary requirements and expenditure approvals.

Project Governance

Governance of ICT projects within Police will also follow the guiding principles of this ICT Strategic Plan and ensure that:

- planning is addressed in an integrated business focused and inter-project manner
- ICT projects and acquisitions follow an approved process to support strategic business initiatives; and
- development of business initiatives leverages the ICT infrastructure.

Project Management Office

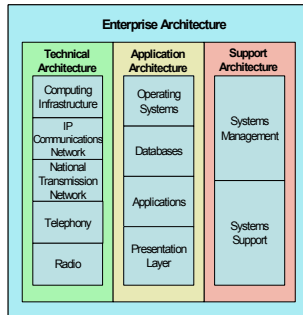
The role of the PMO is to provide an independent overview of the programme of major projects. This includes validation of scope, business case, project schedules and costs. The PMO monitors project progress and reports to the Police Executive.

Business as Usual Governance

Governance of business within the ITSC will conform with Police regulations, policies and procedures; including the ICT architectural and operational rules.

5. ICT Strategy

The Systems Architecture is the “rules of the game”. The Systems Architecture defines the standards to which the technology and applications will be designed, built, maintained and replaced.



The Police Information and Technology Service Centres manage a large and diverse IT infrastructure and application environment. Key features include:

- Over 6,500 computers and 1650 printers in sites from Kaitaia to Bluff and the Chatham Islands
- IT management of one of New Zealand’s largest private networks for data and voice communications
- the enterprise data network reaches over 380 police stations and exceeds the 99.9% SLA target availability
- 10,500 desk phones on a virtual private network, complemented with 2400 cellphones
- over 300 radio sites feeding real time communications to over 2,500 vehicles, foot patrols and stations over 3,000 handheld radios
- high network utilisation and information system transaction volumes
- both commercially available and Police developed applications.

Also refer:

Appendix 1:
ICT Strategic Plan Review and Update Process

Appendix 2:
Progress Since Last ISSP

Systems Strategy

Systems will employ a common architecture and will be built and managed consistent with industry best practice, applicable standards and associated methodology.

The systems infrastructure will be designed, developed and built on the principles of open systems based, standardised, integrated, secure, robust, scaleable, supportable, fit for purpose, cost effective and licensed systems.

Applications will move to a single entry (utilising multiple input devices) and single place of storage (with business continuity) to provide information for knowledge based decision making at the point of action, anywhere, any time.

Police will use industry recognised standard methodologies and toolsets to govern system selection and application development processes, from business requirements through design; build; unit, system and integration testing; to training, support, production and business continuity.

Technical Strategy

End User Computing Hardware Strategy

All equipment and systems will be integrated into the computing infrastructure. It is accepted that special operations may require the use of temporary standalone equipment and systems, but these will also meet Police ICT standards.

Computing Infrastructure

Technical environments for critical applications will have either three (for external to Police developed applications) or four (for Police developed applications) physical environments, being Development, Test, Production and Business Continuity / Disaster Recovery.

Multi Service IP Network

Police will continue to use IP Protocol and consolidate remaining non-enterprise networks into an integrated voice, video and data transport network.

National Transmission Network

Because of the growth in overall network traffic, Police will continue to expand the Police owned microwave network to provide additional capacity and redundancy.

Telephony Infrastructure

Police will migrate the telephony network to Internet Protocol (IP), and converge voice and e-messaging with remote working applications to provide structured access to Police for first responder, routine and administrative services.

Radio Infrastructure

Radio remains the primary voice communication channel for frontline policing. Police will progressively migrate the analogue conventional radio infrastructure to APCO25 IP based digital encrypted conventional/trunked infrastructure operational communications.

Wireless Connectivity

Police will use the public network to transport information to the mobile workforce. Secure gateways, two-stage encryption and VPN technology will be used to provide secure connectivity and protect the integrity of information.

Over the last four years Police has invested to refresh servers, workstations, desktops, laptops, printers, scanners, network components, radio equipment and telephony equipment. These items are now subject to an ongoing annualised equipment refreshment programme.

The key benefit of this work has been to provide Police with a modern communications and computing infrastructure and effective business applications to capture and enter information accurately. This provides the base on which to build the new initiatives proposed in this plan to further improve the effectiveness of Policing resources.

“We could not do what we now plan to do, if we hadn’t done what we’ve done.”

Refer:

Appendix 3:
Ongoing ICT Enterprise Refresh

ITSC provides Police with 24 x 7 access to a suite of applications that enable policing through providing shared and secure communications, knowledge, intelligence, decision support and performance reporting.

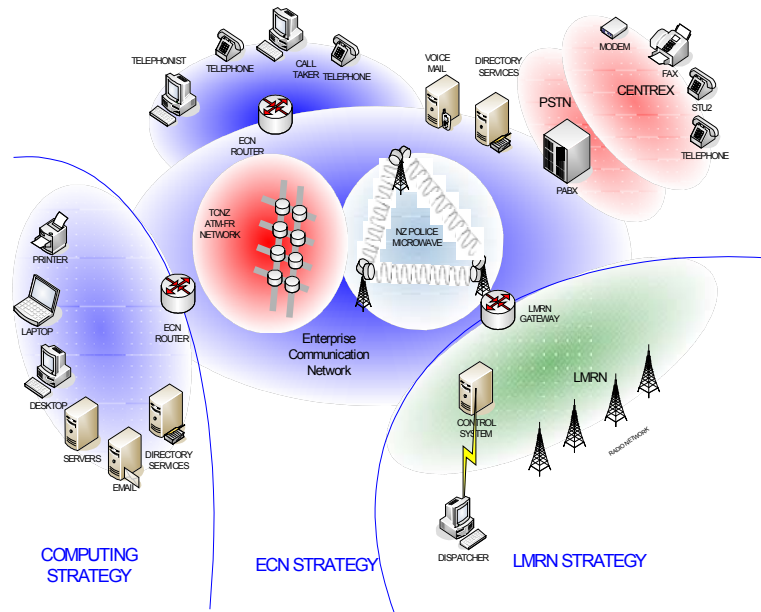
Over 1.6 million calls are received each year; of which 466,000 are 111 calls.

12% of 111 calls are Priority 1, requiring a 0 to 10 minute response.

77% of 111 calls are Priority 2, requiring a 0 to 30 minute response.

Police process over 30,000 scene of crime and 90,000 prisoner fingerprint samples per annum. The fingerprint database contains over 570,000 samples.

The Police technical infrastructure components are shown in the following diagram:



Application Strategy

Operating Systems

Police will continue to utilise current versions of Microsoft and Sun Operating Systems.

Databases

Within the enterprise environment three database types are used, being DB2, Oracle and Microsoft SQL Server.

Applications

Required functionality is provided through approximately 60 commercial and Police developed applications. These will be reviewed and rationalised under a programme of systems interfacing and integration.

Communications and Resource Deployment (CARD)

A number of 3rd party and in-house developed applications are interfaced to support the communications, command and control functions of the three Communications Centres, located in Christchurch, Wellington and Auckland. Emergency and routine calls for service are answered by call takers and assigned to dispatchers to deploy response units according to service priority. To assist decision making CARD provides nationwide maps showing road names, address points, raster and aerial images, caller line identity and location and status of response units. Systems are kept current with regular updates of core mapping, address and telephony information.

Automated Fingerprint Identification System (AFIS)

A commercial comparative fingerprint processing and analysis system used nationwide for proof of identity purposes.

Over the last three years Police have placed the majority of applications development effort into the LES to NIA migration. Police recognise that going forward there will be a more balanced workload between large and small application development projects. With the delivery of the major modules of NIA it is expected that the application update programme will comprise twice per annum releases of NIA upgrades and regular updates of smaller applications.

With over:
 9,700 FTE Staff,
 20,300 million hours and
 \$1,015 million in funding appropriations; Police applications support high volumes of complex transaction processing, 24 x 7.

Typically, over:
 477,000 Personal vetting
 120,000 Property
 162,000 Apprehension
 240,000 Bail & parole check
 183,000 Crime related
 241,000 Incident related
 447,000 Investigation
 122,000 Prosecution
 145,000 Court document
 125,000 Prisoner
 24,000 Drink/drive offence
 66,000 Vehicle restraint, and
 87,000 Traffic emergency events per annum are supported by multiple transactions per event.

National Intelligence Application (NIA)

This is an in-house developed records management application and is the primary operational policing system supporting the intelligence gathering, investigation and prosecution functions of Police. NIA interfaces to other justice sector agencies for the transfer of offence related information.

Criminal Investigation Database (CID)

CID is a commercially available package that provides a highly secure capability, for the management of complex and / or long-running criminal cases and special operations. CID has sophisticated entity relationships and text management capability.

I2

The ANACAPA standard compliant primary intelligence application used by Police Intelligence sections for the linking of data associated with large investigations and operations.

MAPS

Is a Police developed spatial database application that supports the extraction of data (events) and the mapping of those events. It is used extensively by Police Intel as a decision support tool.

Human Resources

Police use a commercially available system to provide support for Police human resources management. The system supports the entering and maintenance of personnel related information and reporting structures. It also provides payroll capability.

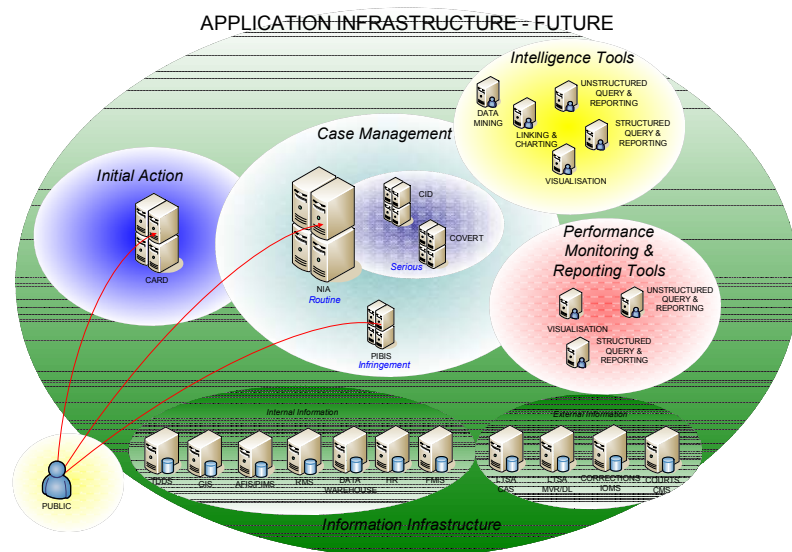
Financials

Police use a commercially available package, providing Police financial management systems including general ledger, asset management, accounts payable and procurement.

Data Warehouse

Corporate data warehouse developed on an Oracle database. Is the central repository for corporate information extracted from Police corporate systems. A commercially available package provides structured query and reporting function capability within the data warehouse database.

The Police application infrastructure components are shown in the following diagram:



Office Automation

Lotus Notes and Microsoft Office applications provide the infrastructure for written communication at Police.

Information and Knowledge Management Tools

Knowledge Management is commonly defined as “enterprise embodying organisational processes that seek synergistic combinations of the data and information processing capacity of information technologies with the creative and innovative capacity of human beings”. Distilled, Knowledge Management is “information in context”.

These will use portal based knowledge-sharing toolsets to provide threaded discussions, document sharing, library database access, and processes organised by templates that let individual communities post and manage Intranet based information.

The Police Intranet will be used as a supplementary system for providing training and certification.

Support Strategy

Strategy objectives of the ICT service delivery model are:

- to support Police achieving the objectives of the “Safer Communities Together” strategy
- provide systems that are available, reliable, appropriate and supported by suitably skilled staff to enable “Policing Together” to meet the Police business requirements
- to provide the services transparently to the Police to maximise Police “public visibility time” available to address community safety
- focus on the “end to end” solution required by the Police, and
- to include clear ownership within the ICT Support team to minimise Police time required within the issue resolution process.

It includes:

- preventive maintenance
- systems monitoring and management
- systems administration
- Moves, Adds and Changes
- System security and performance.

It also includes rollouts of, upgrades to and refreshment of ICT equipment, operating systems, databases and applications.

The ITSC provides, from a catalogue of products and services, ICT support to Police business units in accordance with mutually agreed SLAs.

Typically this work is about responding to planned and unplanned Police operational requirements and ensuring ICT systems availability and performance exceed the SLAs. This is an essential category of work and priorities in this area, driven by supporting Police operational requirements, will generally supersede all other ICT work priorities.

All requests for ICT service are directed to the NZ Police Help Desk. Requests are managed utilising the HEAT help desk application. Service requests are issued to either in-sourced or outsourced support services. The same measurement matrix for performance reporting is used for all SLA performance reporting.

Support work carried out “in-house” includes support of:

- LMRN microwave
- MAPS, and
- the Data Warehouse.

Support work outsourced includes support of:

- Telephony
- the Data Network
- CARD, and
- AFIS.

Where outsourced service providers are used Police have back-to-back SLAs with those providers. Each supplier of outsourced services has their own service management system with links to the Police HEAT system.

Police have also entered into a partnering approach for all architectural design, development and support of the NIA and CID applications.

System Management

Police use the Tivoli suite for enterprise wide system management.

Police plan to achieve:

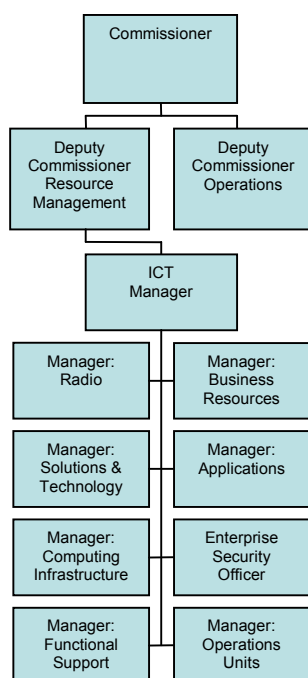
- Total of in-process calls less than 2 days average call volumes
- 65% resolved same day
- 71% resolved by Day 2
- 80% resolved by Day 7
- 88% resolved by Day 14
- 94% resolved by Day 21
- 100% resolved by Day 100.

Police recognise that both climate and geography will affect request for service in some instances.

Typically there are over 200 tasks in process at any time in the Master Work Schedule.

Police must meet legal and statutory requirements regarding the security of both data and the systems/network. To this end Police have procedures regarding physical and/or electronic access to the Police infrastructure, equipment and data. These are based on applying industry best practice in accordance with the manual *Security in the Government Sector* and *AS/NZ ISO/IEC 17799*.

Organisation of NZ Police ICT



Systems Support

Police provide

- an internal 24 x 7 Help Desk for Police staff, for first call registration, initial diagnosis and resolution of all ICT related issues
- 24 x 7 monitoring of the all critical infrastructure and applications
- application support for Police developed applications and first level application support for Partner/Vendor supplied applications during normal business hours
- onsite repair of computer, telephony, radio and communications hardware, on either a replacement or rebuild basis, and
- a business continuity and disaster recovery environment.

Work Management

Work is formally assigned to ICT staff and work managed using a “Master Work Schedule”. All projects have a sponsor group, a business owner, a technical owner, a project manager, a support owner and an implementation team leader. While projects are managed individually, the overall work plan is tracked and coordinated by work stages; being Initiation, Planning, Execution, Commissioning and Completion.

Security Strategy

A key function of ITSC is to maintain the security of Police ICT systems, protecting Police’s information assets and ensuring confidentiality, integrity and availability requirements are met.

Systems will be subject to regular standards compliance audit. If risks are identified they will be assessed in accordance with the Risk Management Standard AS/NZS 4360:1999. Risk mitigation plans will be executed dependent on the risk impact assessment.

Document and information security will comply with the Security in the Government Sector (SIGS) national information classification system. Information codification, storage and retrieval systems will comply with SIGS standards.

ICT Human Resource Management Strategy

Succession Planning

With a relatively small and long serving ICT team there is a potential issue regarding succession. Succession planning is therefore critical. Staff skill development will specifically target this need. Where suitable expertise can not be provided from within Police it will be sourced from external sources.

This is especially so in the radio area, where there is not a ready pool of expertise outside Police to recruit from. Therefore Police will provide a career path based from direct entry through to senior technician level, with progressive training provided by Police and partner training establishments.

Skills Development

Police ICT will spend 5% of salary related expenses on staff training and development. All training and development undertaken by Police ICT staff must be relevant to the person’s role and future career path within Police. All training and development time and associated expenses must be approved prior to being incurred.

User Training

In conjunction with the Police Training Service Centre, ITSC will ensure the provision of appropriate ICT infrastructure, application and systems training to Police staff, dependent on their role.

6. User Strategic Themes

Policing enabling strategic business related themes were confirmed during Police user representative new initiative prioritisation discussions. The user strategic themes are:

Improve Service Access for the Community

Police want to enable more effective communication methods with the community. This will focus on improving current methods together with providing alternatives for the community to communicate with the Police.

Reduce Repetitive Paperwork

Police want to simplify the data input process and remove repetitive entry of common data (“Enter once”) when completing standard transactions.

Improve Integrated Reporting

Police want to standardise repetitive report formats, so that key information can be system generated. This will require simplification and consistency of event coding and data storage, so that consistent and comparable hierarchical reports can be generated organisation-wide.

Maintain Security and Integrity of Information

Police must ensure information in their care is true and appropriate to hold, and that formal security information levels are correctly applied to that information. These dictate data storage and access rights criteria which must be strictly managed.

Improve Intelligence

Police work to an intelligence led policing model. Key to this is constantly improving intelligence gathering, compilation, analysis, presentation and resulting decisions. Enabling technologies have a key role in this regard.

Improve Investigations

Investigations are a core component of policing work. Police look to using technology to both enable and improve the effectiveness and efficiency of this work.

Improve Deployment

Police constantly have to balance personnel resource availability with demand. This requires instant knowledge of resource location, status, skills of deployable staff; locally, regionally and nationally.

7. ICT Strategic Technology Themes

ICT Strategic Planning workshops with vendor partners, together with discussions with other law enforcement and government agencies, identified seven ICT strategy related themes:

Mobility

Police are a mobile workforce and require realtime access to all Police systems either when at a Police site, in a Police vehicle or even from home. The Mobility initiatives in this strategy are about providing access in a secure way, while protecting the integrity of information.

Dimensional

Intelligence-based Policing requires the provision of systems to analyse and predict crime and crashes by event, time and location. Providing modern graphical and spatial-based toolsets will provide for intelligence-based interventions to occur and so deter crime and crashes.

E-Learning

Increasing public demands on Police time and requirements to remain compliant with Police certification requirements mean a change to the methods Police have traditionally used for training and knowledge sharing.

Providing computer-based training courses and video-based methods of communication will, in many instances, allow faster knowledge sharing with less travel.

Case Management

Police have many stand-alone applications that constitute the system currently used to manage cases and associated events from initial public request or advice through to completion, often presentation at court. Police will seek more interfaced and integrated systems and processes to effect case management.

Systems Integration

Police require access to multiple databases within and external to Police. Police also have multiple systems currently providing, and others capable of providing, given functionality. This leads to a multiplicity of information sources. Police will work to consolidate systems and databases with the objective of single data entry and single storage points and removing duplicity of application functionality.

Business as Usual ICT Refresh

Police recognise that, even if no new projects are undertaken, the current infrastructure will continue to be subject to constant refreshment and ongoing updates and improvement. Budget provision for the ongoing annualised investment required to maintain the currency and capacity of the existing infrastructure will be budgeted for annually, separately from the projects that add new capability to the Police ICT environment.

Improved ICT Support Service Delivery

Police have a significant investment in infrastructure and systems. It is the role of the ICT Service Centre (ICTSC) to provide maintenance to these. In this regard user support is paramount. Police will undertake a programme to enhance the service culture within the ICTSC to consistently meet industry best standard service levels.

8. New Initiatives

Eighty-six potential new initiatives to increase policing capability were developed from consultation with Police user representatives, vendor partner workshops, discussions with other justice sector organisations and law enforcement agencies and desk research.

While business-need driven, the new initiatives were also grouped by ICT theme to enable identification of solution sets. This will enable solutions to be designed and implemented which address groups of related business requirements, rather than single point solutions.

Refer Appendix 4: Business Initiatives

The new initiatives were ranked in importance by representative Police user groups. This output has been used to confirm prioritisation for implementation of the new initiatives, commencing with the “Top 10”.

The Top 10 new initiatives are:

- Encrypted radio communications
- Car as a Police station
- Case management
- Improve identification – fingerprint capture & check
- “Standard Reporting” – starting with timesheets
- E-Query
- Automated vehicle location & GPS
- Non-emergency contact number, e.g. 0800 311 311
- Improve data capture and quality in the field, and
- Improve identification – Automated Number Plate Recognition.

Refer Appendix 5: Prioritised Business Initiatives by User Strategic Theme

9. Workplan

Police continue work on the Business as Usual infrastructure refresh and have commenced work on:

- Programmes to address the Top 10 initiatives, and
- ITSC service delivery improvement.

The Top 10 initiatives, by user strategic theme, are:

A. Improve Service Access for the Community

Non-emergency contact channel – phone

Police will provide nationwide 24 x 7 non-emergency voice channels for the community to contact Police, e.g. a 311 or 0800 based service. This will provide a separate direct contact option for the community for non-emergency calls allowing the Communications Centres to address service priorities. The objective of these alternative channels is to ensure the 111 priority service is focused on emergency calls, is not adversely affected by non-emergency calls and that emergency resources and equipment are targeted to provide the contracted response levels to the public.

B. Reduce Paperwork

Car as Police station & beat access to core Police applications

Police will implement an enabling project to provide nationwide frontline mobile access to and interaction with Police systems, based on a police car being equipped with computing infrastructure to access core policing applications and functionality, commencing with response unit status, QVR and QP. This will improve the effectiveness and efficiency of core repetitive policing functions and also reduce load on the radio network and Communications Centres.

E-Query

Where the cellular network provides coverage, provide frontline staff proactive remote field access to E-Query (QVR / QP), using secure handhelds, in order to remove repetitive general communications traffic from the Communications Centres, using technology to automate the response to queries.

Improve data capture and quality in the field – eliminate repetitive data input

Use standardised forms nationwide to eliminate repetitive input, improve workflow, quality of data and downstream collection and analysis of statistical information to meet statutory and organisational reporting requirements.

C. Improve Intelligence, Investigation & Deployment

Case Management System

Scope a nationwide case management system to improve:

- effectiveness and efficiency of Police in crime solution and reduction
- conformance to information security and integrity standards
- communication of information, both internally and externally
- allocation and coordination of resource and prioritisation of workload, and
- Management of the overall caseloads.

Improve identification – Fingerprint capture & check (Livescan)

Provide for police station and nationwide mobile computing “point of action” capture, upload and comparison of fingerprint and receipt back of identity information to confirm proof of identity for persons of interest, so enabling identification of persons of interest with outstanding warrants/fines and reduction of crime.

Automated Vehicle Location & GPS

Ongoing rollout to provide location information of a resource (vehicle or a unit/person) using the GPS facility, forward and interface this information with the CARD system. Resource location information will be displayed to Communications Centre operators and other staff who need to know the location of resources. This will increase officer safety, improve deployment of resources and confirm adherence to the vehicle pursuit policy.

Improve identification – Automated Number Plate Recognition

Pilot to provide fixed and mobile ANPR facility to enable identification of vehicles of interest, especially stolen vehicles. Initially provide on-line ANPR functionality in ACC Stop buses.

D. *Improve Integrated Reporting Systems*

Standard Reporting – Starting with Timesheets

This is a programme of work to simplify coding and standardise formats of repetitive management and performance reports across districts to:

- Enable consistent presentation and source comparable management information
- Standardise inputs and minimise custom reports
- Provide more comprehensive qualitative reports
- Allow true aggregation of information, and
- Improve response and minimise reporting cycle,

commencing with the Activity Management System (AMS) to provide on-line access to staff, simplifying the timesheet process, automating allowance claims and providing for the creation of static rosters.

E. *Security and Integrity of Information*

Encrypted radio communications

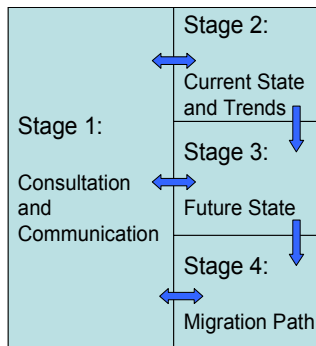
In conjunction with the introduction of the digital trunk radio network to progressively provide nationwide encrypted radio communications to improve security and confidentiality of Police radio based communications. This will be a long term project, commencing with implementation for specialist groups and areas with critical operational pressures.

ITSC Service Delivery Improvement

The Police ITSC has Service Level Agreements (SLAs) with Police business units. To ensure service delivery performance meets Police requirements the ITSC will:

- align all individual area measurements with key customer requirements, that is “professionalism”, “earliest resolution” and “fixed for ever”
- improve visibility of service results against the above key customer requirements
- continue moving from a reactive to a proactive service delivery environment
- review and simplify all reporting and fault recording processes, and
- monitor individual performance of ITSC staff and identify areas for improvement and training and development opportunities.

Appendix 1 ICT Strategic Plan Review and Update Process



A four-stage methodology was used to develop the ICT Strategic Plan:

- consultation and communication
- confirmation and definition of current state and trends
- defining the future state
- defining the migration path

Stage 1: Consultation and Communication

Throughout the development of the ICT Strategic Plan a programme of consultation and communication with representative stakeholders was undertaken. This programme sought input and tested the formation and refinement of ideas and initiatives with Stakeholder groups on an iterative basis as the ICT Strategic Plan was developed.

Stage 2: Confirmation and Definition of “Current State” and Trends

The initial phase of developing the ICT Strategic Plan included four parallel streams of work:

- a review of current Police Strategic Plans:
 - Police Strategic Plan to 2006
 - People in Policing: a Five Year HR Strategy to 2006
 - Road Policing Strategy 2001-2006, and
 - the 2001-2004 ISSP
- workshops with ICT strategic partnerworkshops with representatives of user groups within NZ Police, and
- the development of the candidate project prioritisation process.

The 2001 ISSP Review

The review of the 2001 ISSP considered:

- the current state of information systems, processes, organisation and knowledge
- progress on projects and initiatives completed to date
- evaluation of ongoing projects, and
- review of projects yet to commence.

These were considered in regard to:

- changes in the international policing environment
- changes in NZ policing requirements
- projected future trends in policing, both internationally and nationally
- current state of technology, and
- proposed and projected advances in technology.

Further Australian, Singaporean, United Kingdom, Canadian and United States of America Law Enforcement Agencies’ strategic plans and ICT Strategic Plans were considered to understand the issues confronting other law enforcement agencies and how they are effecting ICT solutions to address these.

ICT Strategic Partner Workshops

During the development of this ICT Strategic Plan over 25 workshops were held with ICT strategic partners. These are vendors who provide core infrastructure equipment, systems or services. The objective of the workshops was to discover technology and business trends and to identify where and how these apply to policing in New Zealand.

Business Workshops

Workshops were held with representative user groups. These workshops considered:

- Police strategic outcomes
- future policing scenarios, and
- offshore policing trends.

The workshops developed views of how ICT can enable policing in New Zealand, from which the list of candidate projects was developed and prioritised.

“Future State” definition enables identification of future information systems & technology, including (at a high level):

- Business models
- Operational processes
- Information & data required
- Support & management processes
- Future information facilities
- Automation opportunities
- Potential problems, and
- Potential opportunities.

Stage 3: Define “Future State”

As a result of the workshops and other research an understanding of the future state was reached. This included:

- confirmation of Police strategic direction and potential changes in business plans
- visioning of future Policing scenarios to 2010
- Technology trends affecting NZ Police
- Best practices in technology, and
- ICT required to support Policing to 2010.

From this work both the ongoing enterprise maintenance initiatives and the new candidate projects were identified. The latter were prioritised by representative Police user groups.

Stage 4: Define “Migration Path”

Police recognise the organisational constraints that apply in both delivering and the capacity of the organisation to absorb major ICT enabled change programmes. Delivery and implementation of these programmes must not diminish the capacity or capability of Police to carry out policing.

Once the prioritised candidate projects business impact, resource, schedule, financial and risk profiles are understood, in conjunction with the existing business as usual and current and previously planned projects, the overall migration path will be confirmed. This work will be ongoing and includes:

- identifying and qualifying possible constraints and overall risks
- determining the optimum purchase and development sequences
- identification of priority projects
- preparation of business cases for priority projects
- confirmation of funding
- confirming the information resources governance processes and management infrastructure, organisation structure and requirements for personnel, and
- the implementation of procedures for ongoing annual updating of the ICT Strategic Plan.

Appendix 2 Progress Since Last ISSP

Since the 2001 ISSP Police have made substantial achievements in the stability of the ICT platforms because of the focus on doing a few things very well. These areas of focus were the:

- Land Mobile Radio enhancements, upgrades and refresh programme
- Computing Infrastructure Replacement programme
- IP Network implementation programme, and the
- LES to NIA application migration.

Also since the 2001 ISSP substantive progress has been made in strengthening the governance, modernisation and integration of the Police ICT infrastructure. ICT work since has focussed on addressing identified risks and completing identified projects, together with implementing works required as a result of legislative changes or Police mandated programmes.

At the time of the 2001 ISSP Police faced some significant infrastructure issues. These dominated business considerations during that ISSP prioritisation process. Addressing these core infrastructural programmes has provided the foundation for enhancing existing and building new solution sets for the current issues Police face. Without the work since 2001 the new initiatives would not be possible. Progress since the 2001 ISSP is shown below.

	Completed
Top Priority	<ul style="list-style-type: none"> • Implementation of an upgraded computing infrastructure of servers, desktops, laptops and printers; including updated operating systems • Porting the mainframe computing environment to an open system server based environment • Server upgrades to the Communications and Resource Deployment (CARD) and Human Resources Information System (HRIS) • Implementation of an advanced IP based, enterprise-wide multi-service network • Implementation of nationwide IP based telephony and messaging, including upgrade of key PABXs • Migration of components of the mainframe-based Law Enforcement System (LES) to the National Intelligence Application (NIA): <ul style="list-style-type: none"> • Firearms, property, message switching replacement • Electronic interface to Department of Corrections • External information interfaces to the Ministry of Justice, the Land Transport Safety Authority, • Document Locator, family violence, INCOFF (Statistics), vehicle related information • Phase 3, detailed design for Phases 4, 5 & 6 of the migration. • Phase 4, Master person related information, Modus Operandi, entry and viewing of charges • Upgrade of the Tivoli computing infrastructure management system • Human resource systems • Provision of encrypted digital radio for Police tactical groups • Implementation of formal project governance
Secondary Priority	<ul style="list-style-type: none"> • Business continuity projects, including significant investment in business continuity and disaster recovery infrastructure • Implementation of enhanced network security infrastructure and management
	In Progress
Top Priority	<ul style="list-style-type: none"> • Land Mobile Radio Network (LMRN)
Secondary Priority	<ul style="list-style-type: none"> • Enterprise Information Store (EIS) • Case management • Covert investigations technology • Communications centre enhancements • Image and document management • Database management system • E-Government and e-Police services
Pending	<ul style="list-style-type: none"> • Video interview systems

Appendix 3 The Ongoing ICT Enterprise Refresh

ICT technical refreshment and updates will be continuous and subject to the Change Control process. Update cycles will typically be:

- Hardware refreshment, for development, test, production and business continuity/disaster recovery environments:
 - Servers – every three years
 - Desktops – every four years
 - Laptops – every three years
 - Printers – every three years
 - Scanners – every three years
- Multi-function photocopier/printer/scanner devices – every three years
- Operating Systems:
 - Standard upgrades on production release from Microsoft and Sun, timing to suit Police operational requirements
 - Service packs and security updates will be tested immediately and installed upon acceptance
- Databases:
 - Standard upgrades on production release from IBM and Oracle, timing to suit Police operational requirements
 - Service packs will be acceptance tested immediately and installed upon acceptance
- Applications:
 - System management application upgrades on production release from IBM, timing to suit Police operational requirements
 - In-house developed applications will be subject to standard six-monthly releases to production
 - Purchased off-the-shelf applications will be upgraded on production release, subject to timing suiting Police operational requirements
 - Additional modules of purchased off-the-shelf applications will be installed following business case approvals and acceptance testing, subject to timing of installation suiting Police operational requirements.
- Networks:
 - Enterprise IP Network: capacity upgrades every six months.
- Radios:
 - Radio upgrades will be subject to the Land Mobile Radio Upgrade project
 - Specific radio groups will be upgraded based on operational unit requirements
- Telephones:
 - Fixed – every seven years
 - Cellular – every three years.

It is noted that maintenance contracts with most technology partners include take-up of technology updates and upgrades during the life of the contract as of right.

While the ICT strategic plan confirms Systems Integration (SI) as a key theme, SI is also a part of the ongoing business-as-usual work. This includes:

- using infrastructure convergence, and other system rationalisation
- ongoing building of interfaces between internal and external systems, and
- consolidation of functionality to provide seamless business processes for users.

Appendix 4 Business Initiatives

Mobility Initiatives

- “Mobility #1” – Automated Vehicle Location & GPS
- “Mobility #2” – Determine alert status of vehicle
- “Mobility #3” – Vehicle Telematics
- “Mobility #4” – Resource log-on from the field
- “Mobility #5” – Automate 3T / Pursuits
- “Mobility #6” – Handsfree
- “Mobility #7” – Improved Voiceless Status Updates
- “Mobility #8” – Scheduler, Contact List and Lotus Notes – Browser Client
- “Mobility #9” – Scheduler, Contact List and Lotus Notes – Full Client
- “Mobility #10” – Voiceless Dispatching for low priority events
- “Mobility #11” – Text Messaging between Communication Centres and Units
- “Mobility #12” – Text Messaging between Units
- “Mobility #13” – E-Query
- Mobility #14 – Field access to NIA: Field Transaction Processing
- “Mobility #15” – Improve data capture and quality in the field
- “Mobility #16” – Improve report process efficiency
- Mobility #17 – Field issue of infringement notices / ticketing
- “Mobility #18” – Digital still camera image capture & upload
- “Mobility #19” – Improve identification – Automated Number Plate Recognition
- “Mobility #20” – Improve identification - Electronic Barcode Capture
- “Mobility #21” – Improve identification – Fingerprint capture & check
- “Mobility #22” – Improve identification – Facial Recognition
- “Mobility #23” – Improve Event location capture
- “Mobility #24” – In-Vehicle Video Camera – Display & Recording
- “Mobility #25” – Portable interview / field reporting application
- “Mobility #26” – Automatic digital traffic camera download
- “Mobility #27” – Field processing of traffic camera infringement notices
- “Mobility #28” – Handsfree operation – Voice recognition
- “Mobility #29” – Field statement - Electronic Signature Capture
- “Mobility #30” – Car as Police Station & Beat access to core Police Applications
- “Mobility #31” – Bail and Warrants
- “Mobility #32” – Portable drugs Testkits
- “Mobility #33” – Self Service Kiosks
- “Mobility #34” – Video Conferencing
- “Mobility #35” – Working from home
- “Mobility #36” – GPS Use
- “Mobility #37” – LMRN/DRN/Encrypted Radio

Dimensional Initiatives

- “Dimensional #1” – Event & Incident “Associations” Intelligence
- “Dimensional #2” – Cars – ‘Stolen’ database (what, where, when)
- “Dimensional #3” – E-Crime – FIU
- “Dimensional #4” – Geocoding
- “Dimensional #5” – GIS
- “Dimensional #6” – Profiling technology
- “Dimensional #7” – Temporal Analysis maps

Case Management and Integration Initiatives

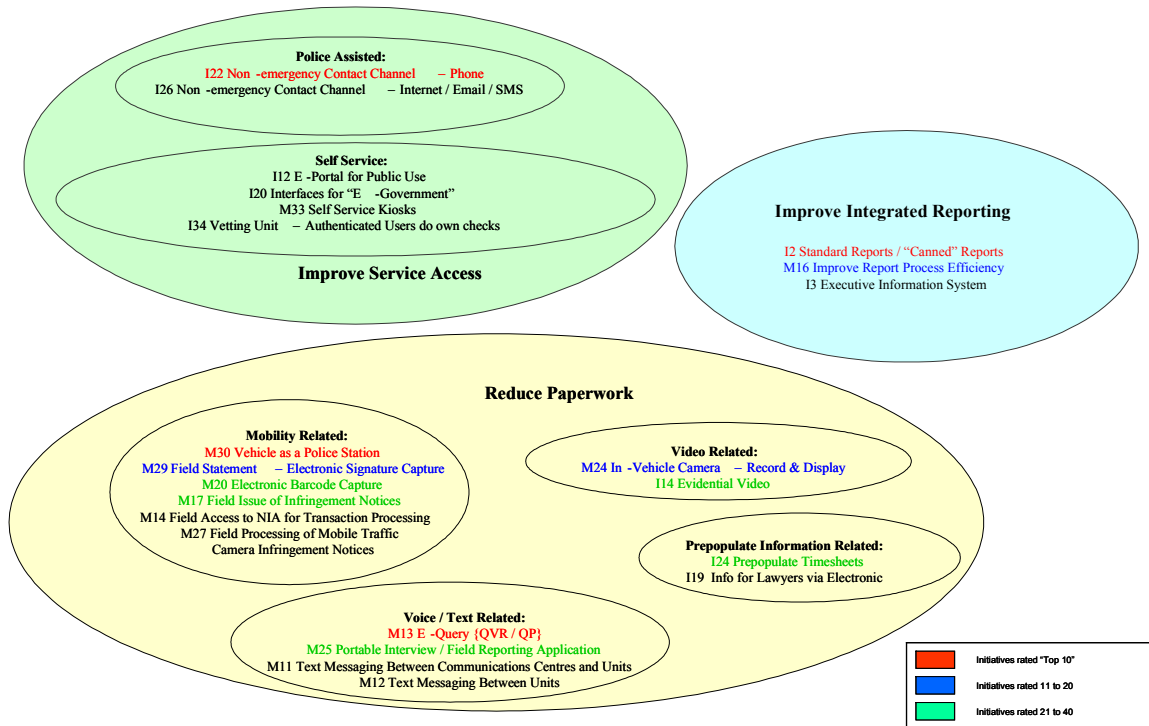
- “Integration #1” - “One Number” Voice and Data Telecommunication
- “Integration #2” - “Canned Reports”/standard reports
- “Integration #3” - Executive Information System
- “Integration #4” - Biometric & Single Signons
- “Integration #5” - Business Workflow
- “Integration #6” - Case Management System
- “Integration #7” - Case Scheduling (Justice: CMS)
- “Integration #8” - Centralisation of functionality
- “Integration #9” - Consolidation of Policing Applications
- “Integration #10” - Document + AV storage and management
- “Integration #11” - Dual entry (avoidance), e.g. Time/Date
- “Integration #12” - E-Portal for use by Public
- “Integration #13” - Evidence Management System
- “Integration #14” - Evidential video
- “Integration #15” - Fines enforcement
- “Integration #16” - Fingerprint for bail reporting in Watchhouse
- “Integration #17” - Home detention
- “Integration #18” - Image recognition technology
- “Integration #19” - Info for Lawyers – electronic
- “Integration #20” - Interfaces and “E-Government”
- “Integration #21” - Knowledge Management
- “Integration #22” - Non –emergency contact channel - phone
- “Integration #23” - Personnel Records – “One Record”
- “Integration #24” - Prepopulate timesheets
- “Integration #25” - Presentation of evidence
- “Integration #26” - Public Non-Emergency Contact System – Internet/Email
- “Integration #27” - Quality Conformance - 7 Elements
- “Integration #28” - Removal of Duplicate Data-stores
- “Integration #29” - Removal of Duplicated Application Functionality
- “Integration #30” - Revisit DR/BC,
- “Integration #31” - SOPS – on line
- “Integration #32” - Streamlining Data Entry
- “Integration #33” - Use of CCTV feeds and records
- “Integration #34” - Vetting unit (Schoolteachers etc) – Authenticated users can do own checks
- “Integration #35” - Voice recognition (Improve Identity Recognition)
- “Integration #36” - Work Planning & Deployment
- “Integration #37” – Voice Based Reporting (Verbal to Written Reporting)

E-Learning Initiatives

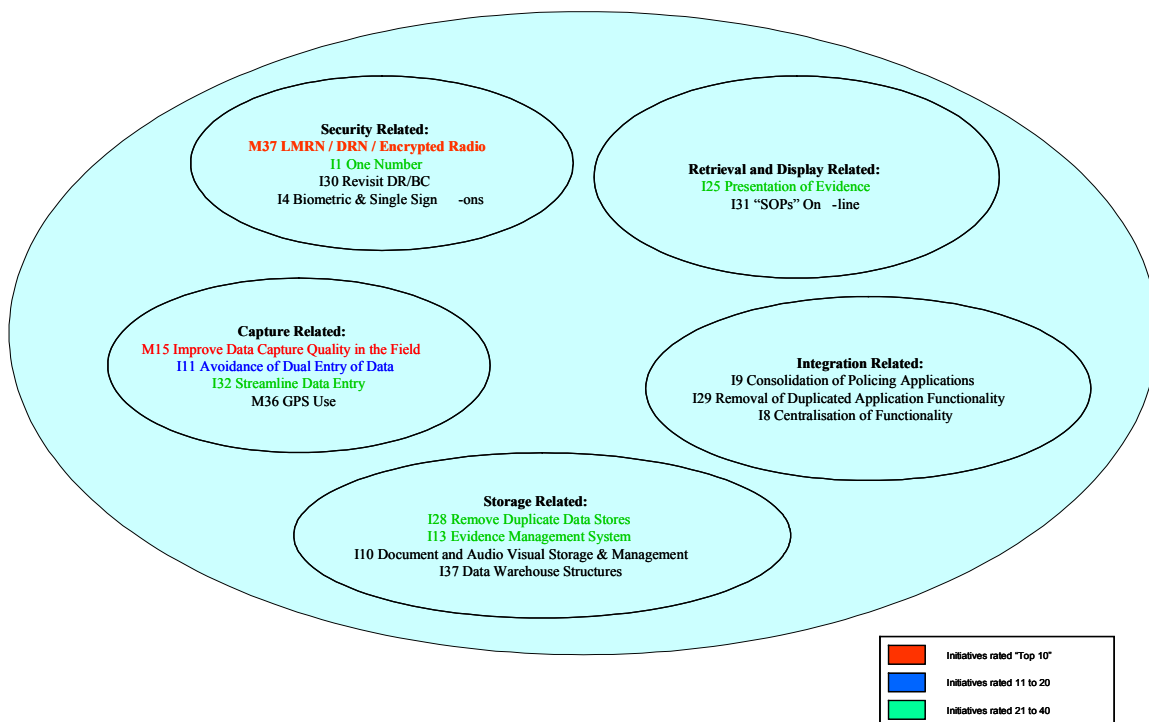
- “E-Learning #1” - Applications: Simulation and Competency Testing
- “E-Learning #2” - Benchmarking – compliance, e.g., ISO 9000, UK – Business Excellence + Some NZ Districts
- “E-Learning #3” - Chat room/Intranet – Knowledge sharing (to help stop reinventing wheel)
- “E-Learning #4” - Communication Campaign
- “E-Learning #5” - E-Training: Computer based courses, assessments and accreditation
- “E-Learning #6” - On line posting of success stories and case studies
- “E-Learning #7” - Real-time Briefing

Appendix 5 Prioritised Business Initiatives by User Theme

Improve Service Access, Reduce Paperwork, Improve Integrated Reporting Systems



Maintain Security and Integrity of Information



Improve Intelligence, Investigations and Deployment

