INDEPENDENT POLICING OVERSIGHT AUTHORITY (IPOA) of KENYA

INFORMATION and COMMUNICATION TECHNOLOGY (ICT) STRATEGY

2013-2018

November 2012

[Purpose of this document 4](#_Toc337817298)

[Executive Summary 5](#_Toc337817299)

[Background 7](#_Toc337817300)

[The Independent Policing Oversight Authority Act, 2011 7](#_Toc337817301)

[IPOA Mandates 7](#_Toc337817302)

[Independence of the Authority 7](#_Toc337817303)

[Objectives of the Authority 8](#_Toc337817304)

[Devolution and Reporting 8](#_Toc337817305)

[IPOA Partners 8](#_Toc337817306)

[General Public 9](#_Toc337817307)

[Civil Society 9](#_Toc337817308)

[National Police Service Commission (NPSC) 10](#_Toc337817309)

[Coroner 10](#_Toc337817310)

[Judiciary 10](#_Toc337817311)

[Community Service Policing 10](#_Toc337817312)

[Police Internal Affairs Unit 10](#_Toc337817313)

[Director of Public Prosecution (DPP) 10](#_Toc337817314)

[ICT Strategy 11](#_Toc337817315)

[ICT Vision 11](#_Toc337817316)

[ICT Strategy Governance Structure 12](#_Toc337817317)

[ICT Executive Committee (ICT-EC) 12](#_Toc337817318)

[ICT Advisory Group (ICT-AG) 13](#_Toc337817319)

[ICT Strategic Pillars 13](#_Toc337817320)

[Hardware Infrastructure 14](#_Toc337817321)

[Data Centre 15](#_Toc337817322)

[Electricity 15](#_Toc337817323)

[Communications, Network, Internet Connectivity 15](#_Toc337817324)

[Security, Physical Access and Monitoring systems 16](#_Toc337817325)

[Desktop PCs, Tablets, Printers, Copiers, Scanners 16](#_Toc337817326)

[Secure Video Conference 16](#_Toc337817327)

[Software Applications and Systems 16](#_Toc337817328)

[Electronic-workflows (e-workflows) 17](#_Toc337817329)

[Decision Support Systems 17](#_Toc337817330)

[Administrative Applications 17](#_Toc337817331)

[Email, instant messaging, office productivity suite (documents, spread sheets, presentations) 17](#_Toc337817332)

[Paperless Office Workflow Applications 18](#_Toc337817333)

[IPOA Website 19](#_Toc337817334)

[Enterprise Resource Planning - ERP (HR, Finance, Asset Management) 19](#_Toc337817335)

[Substantive Systems 19](#_Toc337817336)

[Complaints Register 20](#_Toc337817337)

[Case Management System 21](#_Toc337817338)

[Case Folder 22](#_Toc337817339)

[Access Rights and Audit Trail 23](#_Toc337817340)

[Tasks and Workflow Reminders 23](#_Toc337817341)

[Offline Data Interfaces 24](#_Toc337817342)

[Business Intelligence (BI) 24](#_Toc337817343)

[Complaints/Case Reporting/Ad Hoc Queries 25](#_Toc337817344)

[Feedback to Complainant 26](#_Toc337817345)

[Surveys 26](#_Toc337817346)

[Statistical Analysis and Offence Trends 26](#_Toc337817347)

[ICT Capacity Building 27](#_Toc337817348)

[Classroom Training, Twinning, e-Learning for ICT professionals 27](#_Toc337817349)

[Classroom Training, Train-the-Trainer, e-Learning, Coach Training for IPOA staff and Senior Managers 28](#_Toc337817350)

[Sustainability 29](#_Toc337817351)

[ICT Strategy Implementation Methodology 29](#_Toc337817352)

[Annex 1 – the Independent Policing Oversight Act, 2011 30](#_Toc337817353)

# Purpose of this document

Todays’ successful organizations rely more heavily than ever before on Information and Communication Technology (ICT) tools and services and the achievement of their mandates greatly depends on how well they were able to leverage ICT throughout their operations.

The Independent Policing Oversight Authority (IPOA) of the Republic of Kenya has identified the role of Information and Communication Technology (ICT) as pivotal to the successful achievement of its operational mandates stemming from THE INDEPENDENT POLICING OVERSIGHT AUTHORITY ACT, 2011 calling for IPOA to provide for civilian oversight of the work of the Police.

The purpose of the present document is to identify and analyse IPOA ICT needs and support the vision for the establishment of an organization of the 21st century.

This document highlights the strategic requirements for a robust and secure ICT hardware infrastructure, a number of specialized software applications and a strong ICT capacity building component that will have to be implemented with essential focus on long termsustainability of IPOA ICT operations.

# Executive Summary

Following the promulgation of the Independent Policing Oversight Authority Act in 2011 by the Parliament of the Republic of Kenya and the establishment of the Independent Policing Oversight Authority (IPOA), IPOA engaged in assessing how the convergence of computer systems, software innovation, faster and cheaper Internet connectivity, wireless and mobile phones technology penetration, greater IT-awareness of the general public could be leveraged to achieve IPOA’s mandates in a more effective and efficient way and plot the establishment of an organization of the 21th century.

The investigation of all deaths and serious injuries caused by a Police officer on duty or as a result of Police action, the receipt and investigation of complaints from both members of the public as well as from Police officers, the investigation of misconduct and recommendations for disciplinary action or prosecution, monitoring of police operations that affect the public, and inspecting of police premises are key operational requirements that can be effectively leveraged by engraining the use of ICT in IPOA dna.

The IPOA vision includes:

* online systems collecting complaints data via website, email, social media, mobile phones, and letters. All complaints are tracked and followed up as relevant with the initiation of a possible investigation, and the creation of cases and resulting case folders, allowing for full audit trail of performed action on each case folder item, along with backup and archiving functions.
* online systems allowing for electronic workflows that capture each step of the mandated processes, from the collection of the complainants’ data through the various recording modalities, to the escalation of the cases to the investigation and prosecution stages, as relevant to each case.
* online systems integrated with comprehensive analysis and reporting tools with the ability to analyse statistical trends and collate data for general public information and parliamentary report submissions.
* online systems allowing for the case folder to be securely submitted to the Director of Public Prosecution for further action.
* secure ICT hardware infrastructure capable of independently hosting all IPOA systems.
* comprehensive business continuity and disaster recovery environments capable to ensure data integrity, confidentiality and security.
* distributed ICT infrastructure providing support to a number of regional offices throughout Kenya with the possibility to quickly and cost effectively deploy new IPOA offices in relevant counties to support permanent physical IPOA presence as and when required.
* continuously enhanced ICT capacity and long term sustainability of all IPOA online systems and related infrastructure
* effective ICT trainings, e-learning, twinning and continuous attention to nurture and develop a strong ICT culture throughout the organization work force.

# Background

## The Independent Policing Oversight AuthorityAct, 2011

The Independent Policing Oversight Authority Act enacted by the Parliament of the Republic of Kenya, provides for civilian oversight of the work of the Police by establishing the Independent Policing Oversight Authority while affirming its functions and powers.

Since its establishment, the IPOA Chairman of the Board and the members of the Board of Directors have been engaging in operationalizing the IPOA mandates and building up the operational policies, structures and budgets for the newly created organization.

## IPOA Mandates

Stemming from the Independent Policing Oversight Authority Act, the key IPOA mandates are as follows:

* To investigate any death or serious injury as a result of contact with the Police including while in Police custodywhich are the result of Police action or were caused by members of the Service while on duty (Section 25 of IPOA Act); the serious injury is to be interpreted to mean serious bodily harm including torture, any sexual offence and an offence against a vulnerable person.
* To investigate any complaint by the public against the Police
* To investigate any complaint by the Police against the Police.
* To inspectPolice premises including detention facilities
* To monitor and investigate policing operations.
* To audit investigations and actions taken by the internal affairs unit of the Police service.
* To monitor policing standards, patterns of Police misconduct and provide learning and feedback.

## Independence of the Authority

IPOA has been established as an Independent Authority and:

(1) In the performance of its functions the Authority shall not be subject to any person, office or authority.

(2) The Authority shall observe the principle of impartiality and rules of natural justice in the exercise of its powers and the performance of its functions.

(3) Every Government officer or institution shall accord the Authority such assistance and protection as may be necessary to ensure its independence, impartially, dignity and effectiveness

(4) No person or body may interfere with the decision making, functioning or operations of the Authority.

(5) Parliament shall ensure that the Authority is adequately funded for it to effectively and efficiently perform all of its functions

## Objectives of the Authority

The Objectives of IPOA shall be to:

(1) Hold the Police accountable to the public in the performance of their functions;

(2) Give effect to the provision of Article 244 of the Constitution that the Police shall strive for professionalism and discipline and shall promote and practice transparency and accountability;

(3) Ensure independent oversight of the handling of complaints by the Service.

## Devolution and Reporting

The Authority is required to devolve its services to the counties in accordance with Article 6 of the Constitution.The Authority is required to comprehensively report to the public and parliament every six months or such earlier period should circumstances require.The report shall include the Authority’s opinion on whether any person, authority or institution has attempted to unlawfully or unduly interfere with the operations of the Authority.

## IPOA Partners

A comprehensive review of IPOA mandates and the identification of main IPOA partners, defined as institutions and bodies with whom the Authority has to interface, has produced the non-exclusive list presented in Figure 1.

To a higher or lesser degree IPOA has to interface with all partners below and any data exchange is to be supported by effective and efficient use of secured technology.

Figure 1



### General Public

IPOA key mandate is to receive and process complaints from the public against the Police. IPOA needs to inform the complainant of the status of his/her complaint and offer statistical data to the general public informing them of offence prevalence in the country. All complaints have to be managed by a Complaints Register System that automates most of the workflows and data collection mechanisms.

### Civil Society

IPOA recognises the advocacy role of the Civil Society in sensitizing the general public towards the IPOA mandates, tools and functions that have been established to help them. Websites, social media and training tools have to be embraced by Civil Society leaders to advocate for the successful achievements of the IPOA mandates.

### National Police Service (NPS)

IPOA shall work very closely with the National Police Service (NPS) to ensure that the NPS is rendering an effective and efficient service to the public in accordance within the spirit of Constitution of Kenya and in accordance with applicable international human rights standards and practices.

### National Police Service Commission (NPSC)

IPOA interfaces with the NPSC on matters of policies and reporting on lessons learned, and recommendations from Police audits. Reporting and tracking of recommendations have to be automated in IPOA’s knowledge management systems.

### Coroner

IPOA requires data exchange on Coroner’s reports to be automated in the investigation case management system.

### Judiciary

IPOA receives complaints, prepares case folders. Once cases are fit for prosecution, data exchange with the judiciary is automated with off-line interfaces to preserve security and confidentiality of the IPOA findings.

### Community Policing Entities

IPOA recognises the important role of the Civil Society in contributing to the investigation of relevant complaints and to the successful collection of all findings and evidence related to specific incidents. To ensure solid chain of custody, evidence preserved by IPOA is to be tracked within the investigation/case management system.

### Police Internal Affairs Unit (IAU)

IPOA needs to closely work and exchange information with the Police Internal Affairs Unit (IAU) so to proceed with its investigation on relevant complaint. Data exchange with the Police IAU is to be securely integrated in the IPOA investigation case management system.

### Director of Public Prosecution (DPP)

IPOA needs to closely work and exchange confidential information with the DPP and any recurrent data exchanges have to be managed by appropriate IPOA secure system modules.

# ICT Strategy

Today, in all successful organizations, ICT represents a resource of strategic importance providing for unprecedented ability to dynamically adapt to ever changing needs and environments.

ICT has come a long way from ring-fencing its role to the support of a set of back-office systems and tools and can now be leveraged to support decision making processes and to increase staff productivity as well as improve the organisation’s impact allowing for economies of scale and effective and efficient use of limited resources.

Since its establishment, the IPOA Board has immediately recognized the need to conceptualize an ICT vision and strategy as one of the most important pillars for the operationalization of IPOA mandates.

The IPOA ICT strategy includes the IPOA ICT vision, the establishment of a lean ICT governance structure and the conceptualization of the strategic pillars at its foundation.

The IPOA ICT strategy is a “living document” that will be continuously revised to reflect new ideas, new requirements with the goal to better support the achievements of IPOA mandates.

## 

## ICT Vision

The IPOA ICT vision includes:

* online systems collecting complaints data via website, email, social media, mobile phones, and letters. All complaints are tracked and followed up as relevant with the initiation of a possible investigation, and the creation of cases and resulting case folders, allowing for full audit trail of performed action on each case folder item, along with backup and archiving functions.
* online systems allowing for electronic workflows that capture each step of the mandated processes, from the collection of the complainants’ data through the various recording modalities, to the escalation of the cases to the investigation and prosecution stages, as relevant to each case.
* online systems allowing for the case folder to be securely submitted to the Director of Public Prosecution for further action.
* online systems integrated with comprehensive analysis and reporting tools with the ability to analyse statistical trends and collate data for general public consumption as well as parliamentary report submissions.
* secure ICT hardware infrastructure capable of independently hosting all IPOA systems.
* comprehensive business continuity and disaster recovery environments capable to ensure data integrity, confidentiality and security.
* distributed ICT infrastructure providing support to a number of regional offices throughout Kenya with the possibility to quickly and cost effectively deploy new IPOA offices in relevant counties to support permanent physical IPOA presence as and when required.
* continuously enhanced ICT capacity and long term sustainability of all IPOA online systems and related infrastructure
* effective ICT trainings, e-learning, twinning and continuous attention to nurture and develop a strong ICT culture throughout the organization work force.

## 

## ICT Strategy Governance Structure

With the current ICT strategy IPOA aims at establishing a lean and effective ICT strategy governance structure setting out the lines of authority, accountability and teamwork among the key players responsible to conceptualize ICT requirements, analyse emerging ICT needs and trends and implement relevant actions to operationalize IPOA ICT strategic pillars.

Key ICT governance structures should include:

### ICT Executive Committee (ICT-EC)

The ICT-EC represents the highest decision making body responsible for the coherent implementation of actions related to the ICT strategy vision statements. The ICT-EC is also responsible to approve ICT investments and budgets.

Members of the ICT-EC should be the IPOA Chairman of the Board (ICT-EC Chair), two designated Board Members, the IPOA CEO and the Director of the Information and Communication Division.

Each member of the ICT-EC Committee must designate his/her alternate.

### ICT Advisory Group (ICT-AG)

The ICT-AG role is to provide advice on major ICT activities and strategic directions. The group reviews relevant ICT initiatives and recommends approvals by the ICT-EC.

Members of the ICT-AG should be the Director of the ICT division (ICT-AG Chair) and all Directors of other IPOA divisions.

Each member of the ICT-AG Committee must designate his/her alternate.

## ICT Strategic Pillars

With the aim to establish a long term sustainable ICT environment capable to support the operationalization of IPOA mandates, the ICT strategic pillars are represented in Figure 2.

IPOA should aim at achieving the complete implementation of all ICT strategic pillars in a phased approach according to the ICT Strategy implementation plan that will be developed in due course.

Figure 2



The IPOA ICT environment should rest on three main pillars represented by the ICT hardware infrastructure, the software infrastructure for administrative and substantive systems and the capacity building pillar in the form of continuous ICT training and learning for IPOA and ICT staff.

The conceptualization of all ICT strategy pillars must be developed and implemented with foremost attention to their long term sustainability in order to achieve efficient and effective use of the human and financial resources dedicated to this area.

### Hardware Infrastructure

To sustain IPOA administrative and substantive systems, appropriate hardware infrastructure should be put in place, an IT Infrastructure capable of independently hosting all IPOA systems. Figure 3 below provides a non-exclusive list of items to support IPOA.

The IPOA ICT hardware infrastructure must be planned with relevant business continuity and disaster recovery (BC&DR) parameters in mind so that a complete risk assessment primarily in terms of preservation of security and confidentiality of the data, its accessibility and protection against total loss is conducted and relevant risk mitigation actions are planned and implemented.

Figure 3



IPOA is a new organisation that is expected to build its own capacity in terms of day-to-day operations for an initial staff contingent estimated at 60, growing in the next few years to up to 300 head count.

IPOA is expected to have a local presence not only in Nairobi headquarters but in several counties across Kenya. Staff located in different geographical sites should be able to operate within the same ICT infrastructure, network, security environment and access relevant administrative and substantive systems as they were located in IPOA headquarters.

Strategically, IPOA should become its own “system hosting provider” as this approach mitigates the risk of external parties to be able to access confidential IPOA information and data hosted through commercial hosting providers.

Given the security concerns (both logical and physical) stemming from the IPOA mandates, IPOA should have in place a robust set of policies and procedures to ensure protection of the data it handles.

#### Data Centre

IPOA headquarters offices should host a local data centre equipped with relevant power supply, network cabling and internet connectivity, cooling systems, fire extinguishing systems, physical security access systems, CCTV etc.

The headquarters primary data centre should be complemented by a secondary (BC&DR) data centre in a separate location capable to take over operations in case of disruptions of any nature occurring in the primary data centre.

#### Electricity

Stable power feeds must be arranged for the data centre and the IPOA headquarters buildings. Local electrical infrastructure needs should be assessed when any new IPOA field office is to be established.

#### Communications, Network, Internet Connectivity

Voice (also Internet Protocol - IP based and mobile) and data communication and the underlying IPOA offices cabling infrastructure are pivotal to the functioning of the organisation. Internet connectivity at appropriate bandwidth levels must be sourced through multiple commercial providers in Kenya to ensure failover and business continuity. Internet connectivity availability in relevant field locations should be assessed and, if not available locally, sourced through dedicated installation of VSat stations.

#### Security, Physical Access and Monitoring systems

IPOA’s mandate to manage confidential information throughout its workflows imposes a special attention on the aspect of IPOA data and premises security to be ensured by underlying technical solutions and monitoring systems. As well as data and networks encryption to ensure protection from cyber-attacks and unauthorised access to systems and information, IPOA security policies should cover for risk mitigation in the area of premises physical access and protection. The BC&DR risk analysis should consider the option of storing information in different locations also from a security perspective.

#### Desktop PCs, Tablets, Printers, Copiers, Scanners

Desktop PCs, laptops, tablets, printers, copiers, scanners are some of the standard hardware that should be available for the day-to-day functioning of IPOA both in headquarters and field locations. Configuration, updates, maintenance policies and procedures should determine the efficient and effective use of the IT equipment listed above.

#### Secure Video Conference

The use of video conference is an effective way to bring local offices and headquarters operations to work collaboratively and is an efficient way to save costs. The IPOA network and connectivity infrastructure should support the use of Video Conferencing over IP.

### Software Applications and Systems

The successful achievement of IPOA mandates is dependent on an efficient and effective deployment of policies and procedures that fully rely on online software applications and systems for their implementation.

IPOA requires two different sets of application/systems that will functionally manage the internal administrative activities of IPOA (internal/external communication, word processing, budgeting, recruiting, pay rolling, book keeping etc.) and the implementation of IPOA substantive mandates (registering complaints, investigating offences, obtaining business intelligence).

Despite the somewhat different technology used to implement such a diverse pool of applications and systems, all IPOA online tools should be designed to work towards a “paperless office” environment. This is achieved through the implementation of electronic workflows that should rely, as much as possible, on electronic signatures and audit trails for the verification of decisions and actions taken by authorised officials.

Another common traits of all IPOAs systems should be the reliance on structured data capturing mechanisms enabling datawarehouse technologies to link data items and provide aggregated and/or detailed information in support of decision making processes.

#### Electronic-workflows (e-workflows)

E-workflows greatly assist in engraining the culture of accountability throughout the organization, and, at the same time, enhance speed and accuracy of the service delivery to the benefit of IPOA internal and external customers.

IPOA software applications and systems should be flexible and easy to maintain and at the same time capable of enforcing online workflows that reflect processes and procedures fostering quality service delivery.

The workflow logic embedded in IPOA systems should enforce standards and accuracy at every step, should allow new staff to be immediately productive and should automatically capture mandatory information in formats that can be re-used and reported on.

The use of e-workflows is pivotal to the achievement of IPOA’s impact on both day to day operations and substantive activities in support of the mandates.

#### Decision Support Systems

Information collected and stored in IPOA applications and systems should be mined by reporting interfaces capable to make connections between disparate set of data even possibly collected for different purposes.

Datawarehouse technologies should be used to cross reference and link information to produce online dashboards capable of integrating data to support the decision making process.

Reporting tools should be used to produce mandatory parliamentary reports and to publish statistical data on the IPOA website portal for general public consumption.

#### Administrative Applications

Figure 5 below provides a non-exclusive list of administrative applications to support IPOA internal day-to-day operations.

##### Email, instant messaging, office productivity suite (documents, spread sheets, presentations)

A standard desktop PC must be provided to each IPOA staff to perform their duties. A standard pre-loaded software suite that include office productivity tools, email, instant messaging, virus scan software must be imaged in the computer hard-disk. For users handling confidential information, local hard disk drives must be encrypted. Remote access to email, workflow applications and shared drives should be provided to selected staff through token based RSA security credentials to be used in addition to standard user names and secure passwords.

Figure 5



##### Paperless Office Workflow Applications

The “paperless office” portal should serve as an employee facing self-service tool to perform a series of workflow-based actions. As an example, the IPOA paperless office portal must be accessed to request recruitment actions, to request an expenditure approval, to record mission requests and approvals, to file requests for petty cash reimbursement, to request and obtain approval for annual leave, to request procurement actions etc. The IPOA paperless office portal should allow for tracking the status of the requests and should have a reminder module that automatically sends email reminders to relevant workflow milestone owners. The portal should reduce reliance on physical movement of paper to obtain relevant signatures and approvals as well as allow prioritisation of work throughout all levels of the organisation hierarchy.

##### IPOA Website

The IPOA website should be the main portal of the organization towards the general public. It must be used as an advocacy tool but also as a portal to access the complaints register system where anybody with a browser and an internet connection could register their complaints. A section of the IPOA portal should be fed by the Business Intelligence system providing the ability to draw reports on IPOA activities, access official parliamentary documentation and review IPOA statistical analysis on Police offence prevalence and trends in the country.

##### Enterprise Resource Planning - ERP (HR, Finance, Asset Management)

The IPOA integrated enterprise resource planning system must become the main tool to support the internal administrative functioning of IPOA. The ERP modules to manage human resources, budgeting and book-keeping as well as asset register and procurement processes should be tightly integrated to provide the ability to review the health status of IPOA internal administrative processes and outputs in support of the operational mandates. The implementation of such a system should also engrain full transparency and accountability for staff in charge of administering IPOA human and financial resources.

#### Substantive Systems

While the set of administrative systems aims at bringing efficiency and effectiveness as well as clear responsibility and accountability frameworks in the internal IPOA functioning, the set of substantive systems identified hereafter should allow the organization to become efficient and effective in achieving results in their main substantive mandate areas.

Using the same e-workflow infrastructure the IPOA substantive systems should register complaints, manage the cases arising from reported complains and report on its investigative results to all identified partners with targeted data exchange policies and procedures.

A list of logical substantive systems IPOA should implement is provided in Figure 6.

All IPOA substantive systems/modules should be built with attention to the absolute requirement for seamless data exchange as well as full integration with regards to data items and their interoperability across systems.

Figure 6



##### Complaints Register

The Complaints Register should support the main data collection mechanism for IPOA and should support a multitude of use cases for the general public and the Police to report to IPOA any Police offences.

The Complaints Register must be able to receive complaints in different formats and modality and should be able to appropriately handle all data capturing mechanisms spanning from a standard webpage displaying the IPOA Complaint form, to a quick sms/mms sent to the IPOA central sms number, to a phone call to the IPOA 24X7 automated voice recording system.

The Complaints Register should be designed to collect basic data in any of the different modality outlined in Figure 7 and with minimal human intervention should be able to integrate additional required information through interfacing with other relevant systems, like the National ID card database, the Police IAU system, Criminal Justice System databases, mobile phone providers databases etc. and possibly perform searches on unstructured data stores and social networks.

The Complaints Register system should then be able to assign relevant weight to each complaint according to pre-defined targeting parameters so to automatically bring to the attention of relevant IPOA managers the list of most urgent and possibly most substantiated complaints. This will not only reduce time-to-action but also have the system, instead of individual IPOA human resources, enrich, to the maximum extent possible, data and weighting across the expected substantial number of complaints received by IPOA.

Figure 7



##### Case Management System

Figure 8 below schematically exemplifies the main component of the IPOA Case Management system.

Figure 8



###### Case Folder

Once substantiated complaints analysed by relevant decision making body in IPOA are to be further investigated, the IPOA online Case Management System should be able to support the initiation of the investigative process and the establishment of an electronic case folder (ECF).

The electronic case folder should be the core repository of all documentation (in all forms) that would constitute evidence to substantiate the grounds for the complaints or otherwise.

The electronic case foldershould be capable of capturing, storing, querying and retrieving

information relating to various objects (individual’s records and pictures, documents,

exhibits, events, places, telephone numbers, photo albums, investigator notes, firearms details, vehicle details, TV report videos etc.).

Any object in the ECF can be linked to other objects within the same case file. For example, details of an individual can belinked to a telephone log, or a vehicle registration number etc.

Such links should enable the Case Management System visualizationmodules to facilitate diagramming/charting the information stored in case files to provide the investigators with a simple picture of the connections that could be further analysed in the interest of the successful outcome of the investigation process.

Association matrix, event flow charts, commodity flow charts, telephone call logs etc. should be part of the basic feature set of the Case Management system visualization module.

###### Access Rights and Audit Trail

While the case folder containing all relevant investigation objects is the core element of the Case Management System, it has to be protected from unauthorized access.

The security model built around the case folder has to reflect IPOA policies, procedures and hierarchical roles and responsibilities of relevant investigation actors as well as being able to link to the extent possible objects and case evidence in an integrated manner to provide the value added to learn about best practices followed in other similar cases.

Access rights and security are key component to be taken into consideration by the IPOA Case Management System and need to be maintained centrally by relevant system Super User(s).

Closely linked to the provision of access rights and the safeguarding of data security, the IPOA Case Management System should also include an audit trail log maintaining record of any actions performed into the system, by which user and when. As well as logging any eventual unauthorized access, a simple audit report would highlight any need to balance resources for certain tasks and therefore also serve as a knowledge management tool in what concerns the best use of human and financial resources.

###### Tasks and Workflow Reminders

The IPOA Case Management System should include a workflow engine capable to track not only the various steps to proceed with an investigation but also should provide for the ability to assign cases for investigation to relevant officials and automatically remind them individually of next milestones to be achieved, of relevant reporting requirements to senior officials, of the need to complete assigned tasks within set deadlines and other compliance requirements they are accountable for.

The IPOA Case Management System should include a native function whereby each investigation official could review in one dashboard all cases assigned to himself/herself and the temporal dimension for the next required milestones.

###### Offline Data Interfaces

The wealth of information available in the IPOA Case Management System should be ready to be interfaced, as relevant, with other systems both providing or receiving data.

Relevant interfaces should be built with the Police Internal Audit Unit so that cases under investigation can be merged with IPOA data. IPOA should be able to access the Police systems and extract data relevant to their investigations.

Other interfaces should be built with the Judiciary so that data on cases for which the IPOA investigation process has been complete, can be brought to the Director of Public Prosecution for consideration and action.

Given the confidentiality of the data in the IPOA systems, data interfaces should be built in an “offline” mode so that access to IPOA systems remain for IPOA employees only, while relevant data that needs to be shared is still exchanged to relevant party through offline encrypted data structures that can be easily downloaded and imported in the corresponding external party system.

##### Business Intelligence (BI)

The IPOA online Business Intelligence (BI) modules should provide for a comprehensive query and reporting component that allow for extracting data and combining it in a way to support the decision making process for a range of internal and external IPOA actors/partners.

The capturing of both current, historicaland trend reports on IPOA mandated areas, the querying of data to establish offence prevalence in different parts of the country, the dashboarding of target indicators across the workflow processes of IPOA operations, the production of standard statistical reports for the use by the general public or by the Parliament of the Republic of Kenya should be all features that the IPOA Business Intelligence modules should be configured to output.

Figure 9 below exemplifies the set of tasks that the Business Intelligence Modules should carry out.

Figure 9



###### Complaints/Case Reporting/Ad Hoc Queries

The IPOA Business Intelligence (BI) module should be able to answer, at a click of a button, some of the standard questions reported hereafter but also be able to provide dashboards with analysis on the status of play of relevant investigation actions as well as the ability to cross-link data in several complaints with a case under investigation, provide suggestion on how to augment evidence related to a specific case from disparate data sources and provide decision making support to IPOA management on the next course of action.

The IPOA BI module should include standard report logic to present information about, for example, how many complaints were reported to IPOA in the last month (semester, year), how many more complaints were reported in comparison with last month (semester, year), how many complaints were reported by the public by geographical location, by complainant age group, sex, how many complaints were reported by offence type, how many complaints were founded and a case folder has been opened in the Case Management System, of the ones under investigation, how many are nearing the completion of the process, how many have been transferred to the director of Public Prosecution (DPP) etc.

Based on data access level of the user of the BI modules, relevant ability to “drill-down” from the statistical information and access online the underlying data, i.e. all individual case folders transferred to the DPP, should be a standard feature of the system.

As well as standard reports and dashboards, the BI modules should allow ad hoc queries both for investigators and statistical analysts who should be able to build their own reporting parameters and work on ad hoc requests for information.

###### Feedbackto Complainant

The IPOA BI module should provide for a dedicated service to inform complainants about the status of their complaint. Customer relation functionalities are pivotal to the effort to build trust in the public and provide a complete service.

The customer relation module should be integrated with the complaints register and allow for the indication by the complainants of their will to be informed about the life-cycle of their complaint. The system should be able to trigger emails/sms/letters when the complaint evaluation reaches each major milestones within IPOA mandated processes.

###### Surveys

One pivotal mandate of IPOA is to report on the perceived level of policing standards and analyze data to surface lessons learned and best practices. One of the main IPOA efforts will be establishing benchmarks against which measure improvements.

IPOA should therefore periodically conduct surveys with the general public and store data received, both for prompt analysis and reporting and for historical pattern detection. The IPOA BI module should allow for the formulation of surveys and questionnaires to be filled in through mobile phones to yield large data set on which enable the data mining features of the system.

###### Statistical Analysis and Offence Trends

IPOA mandate to learn about the policing standards and recommend ways to improve cannot be accomplished without technological support to the statistical division. While IPOA is expected to collect large volumes of data, the BI module, using datawarehousing technologies, will have to produce statistical data analysis and reporting.

The BI module should allow for statistical analysts to query data and validate relevant thesis on offence prevalence, on past trends and future trends prediction, perceived effects of changes introduced in the policing standards, impact of IPOA work across the country etc.

### ICT Capacity Building

Pivotal to the overall achievements of IPOA is the effective and efficient use of ICT and pivotal to the effective and efficient use of ICT tools is a strong commitment of the organization to continuous ICT learning that needs to reach all levels of the organisation.

ICT capacity building is a continuous effort and an investment that bear fruits in the medium and long term and should be targeted to different user groups including the ICT professionals who require in-depth technical knowledge of IPOA systems and software architectures, the IPOA super users group who would require targeted, on the job ICT training on systems advanced features and the staff at large who require ICT to perform their duties.

Special ICT training should be planned for IPOA Senior Management in the form of one-to-one coach training and attendance should be made mandatory on a periodic basis.

Relevant training courses should be mandatory for relevant staff according to their functions and should include a certification programme to recognise the level of knowledge and proficiency. The achievement of ICT certification should be linked to financial incentives and peer-to-peer recognition.

Figure 10 highlights some of the main tools and programmes that should be part of IPOA ICT capacity building efforts.

#### Classroom Training, Twinning, e-Learning for ICT professionals

A specialised IPOA team should be selected and trained on the running and maintenance of the IPOA systems to ensure long-term sustainability and ownership of the IPOA operations with limited reliance on external ICT providers.

While the numeric consistency of the IPOA ICT technical team should be estimated according to the phased implementation plan of the present strategy, roles and responsibilities should match a continuous ICT specialized technical training curriculum which includes external classroom based software vendors’ proficiency certification programmes as well as the possibility for on the job twinning opportunities and of course access to e-learning resources available on the net.

Figure 10



#### Classroom Training, Train-the-Trainer, e-Learning, Coach Training for IPOA staff and Senior Managers

A complete ICT certification programme should be established for all staff in IPOA targeting the function of each individual position. The ICT capacity building programme matrix should consider a basic (white belt) level of ICT certification that all staff should achieve and build additional certification levels (yellow, red, green, brown, black belt) that would progressively specialise and concentrate in providing relevant knowledge to perform more effectively and efficiently in each staff member function.

ICT training should be mandatory for all IPOA staff at all levels through an appropriate mix of classroom training, e-learning and coach training. ICT knowledge attained through IPOA ICT certification exams should be considered at time of staff promotion and incentivized with financial rewards linked to the ICT proficiency level attained.

## Sustainability

Sustainability is defined as the capacity that IPOA will have to possess in order to achieve successful implementation of any ICT tools that are designed to be operational for a conspicuous temporal horizon.

All implementation actions stemming from the present ICT strategy should consider their long term complete sustainability as paramount both in the planning and roll-out stages.

ICT sustainability is directly and very tightly related to the ability of IPOA to recruit ICT staff who are committed not only to their role in IPOA but to IPOA goals and mandates.

Given the security and confidentiality of the information that will be handled in IPOA systems, ICT sustainability will extend not only the number of ICT staff that are manning IPOA systems but also to their integrity and long term commitment.

Consideration on ICT system sustainability will have to extend to the careful consideration of their implementation options. Outsourcing and insourcing strategies will have to carefully balance IPOA’s paramount interest to remain independent to the maximum extent possible from external factors as well as being able to make the best use of ICT tools and systems in the context of its mandates.

# ICT Strategy Implementation Methodology

The IPOA ICT strategy should follow a sustainable implementation methodology that should be always incremental instead of “big bang” and consider at every planning stage IPOA internal and/or external customers’ ability to move towards the next milestone deliverable.

The virtuous ICT strategy implementation cycle should include the following:

* Feasibility and assessment study, business requirements definition, and design of the IT infrastructure and software system modules implementation/enhancement
* ICT infrastructure implementation/enhancement
* Software application module implementation/enhancement
* Software feature general announcement, documentation, training, and stabilizing phase support
* Ongoing maintenance and support

The IPOA ICT strategy should be operationalized through a comprehensive and detailed implementation plan.

ss

# Annex 1 – the Independent Policing Oversight Act, 2011

The IPOA Act key statement with impacting the ICT Strategy are as follows:

***“The functions of the Authority shall be to-***

*(a) investigate any complaints related to disciplinary or criminal offences committed by any member of the Service, whether on its own motion or on receipt of a complaint, and make recommendations to the relevant authorities, including recommendations for prosecution, compensation, internal disciplinary action or any other appropriate relief, and shall make public the response received to these recommendations;*

*(b) receive and investigate complaints by members of the Service;*

*(c) monitor and investigate policing operations affecting members of the public;*

*(d) monitor, review and audit investigations and actions taken by the Internal Affairs Unit of the Service in response to complaints against the Police and keep a record of all such complaints regardless of where they have been first reported and what action has been taken;*

*(e) conduct inspections of Police premises, including detention facilities under the control of the Service;*

*(f) co-operate with other institutions on issues of Police oversight, including other State organs in relation to services offered by them;*

*(g) review the patterns of Police misconduct and the functioning of the internal disciplinary process;*

*(h) present any information it deems appropriate to an inquest conducted by a court of law;*

*(i) take all reasonable steps to facilitate access to the Authority’s services for the public;*

*(j) subject to the Constitution and the laws related to freedom of information, publish findings of its investigations, monitoring, reviews and audits as it sees fit, including by means of the electronic or printed media;*

*(k) make recommendations to the Service or any State organ;*

*(l) report on all its functions under this Act or any written law; and*

*(m) perform such other functions as may be necessary for promoting the objectives for which the Authority is established.****”***

***“Lodging of complaint and investigation:***

*(1) A person wishing to lodge a complaint against the Police may do so orally or in writing or in such other appropriate format as may be prescribed in the regulations.*

*(2) Where a complaint is made orally, the same shall be reduced into writing by the employee of the Authority with whom it is lodged, and that employee shall render all reasonable assistance to the complainant to ensure that a proper investigation of the complaint is done.*

*(3) A complaint made under subsection (1) shall contain such particulars as the Authority may from time to time prescribe.*

*(4) Upon receipt of a complaint the Authority shall forthwith—*

*(a) call for information or reports regarding the complaint from the appropriate Government department or agency or any other body within a specified period; or*

*(b) without prejudice to paragraph (a), initiate such inquiry as it may consider necessary, having regard to the nature of the complaint and taking into account the fundamental rights and freedoms of the individuals concerned, including members of the Police , contemplated in Chapter Four of the Constitution.*

*(5) If criminal proceedings are instituted against a member of the Service in respect of a matter under investigation by the Authority, the Authority may suspend its investigation until the conclusion of those proceedings, after which it may continue its investigation or in appropriate cases, decide to discontinue.*

*(6) In the event of the Police having conducted and concluded an internal investigation or internal disciplinary proceedings, the Authority may in appropriate cases and in its sole discretion decide to abide by the outcome of such investigation or proceedings and adopt the findings and recommendations of that investigation or those proceedings as its own, and conclude its own investigation.*

*(7) The Authority shall during an investigation consider the —*

*(a) circumstances which, if present during the incident under investigation, impede the effectiveness of policing; and*

*(b) unlawful action, if any, taken by the complainant, the victim or any other person present during the incident under investigation.*

*(8) Where the Authority considers a complaint to be vexatious or frivolous it may refuse to conduct an investigation.*

*(9) The Authority may upon receipt of new evidence re- open any investigation which has been concluded, and may amend or withdraw any previous findings and recommendations.*

*(10) Nothing in this section shall prevent an individual Police officer from lodging a complaint, but the Authority may, at its discretion, refer any complaint back to the Internal Affairs Unit of the Service for redress.*

*(11) No member of the Police shall be subjected to disciplinary hearings or other disadvantage based solely on the fact that such member has lodged a complaint with or given evidence or information to the Authority.*

*(12) Any person who subjects a Police officer to a disciplinary hearing or other disadvantage based solely on the fact that he has lodged a complaint with or given evidence before or information to the Authority, commits an offence.*

*(13) Nothing in this Act shall prevent any person or body from lodging a complaint in terms of this section, or the Authority from conducting an investigation, even if the target, victim or witness of the action does not agree to or approve of such an investigation by the Authority.*

*(14) Any law providing for the unlawfulness of—*

*(a) the intimidation, harassment or interference with witnesses or potential witnesses to any matter under investigation by the Authority; or*

*(b) concealment, destruction, tampering with or removal of evidence relevant to any matter under investigation by the Authority,*

*shall apply with necessary modifications to the proceedings of the Authority.*

*(15) Notwithstanding any other written law, any document or statement drafted or made or taken during an investigation shall remain confidential until the Authority in writing determines otherwise.*

*(16) The Authority shall upon request from a complainant keep the complaint’s identity confidential unless it is demonstrably in the interest of justice not to do so, until the investigation has been concluded:*

*Provided that the Authority may in exceptional cases determine that the identity of a complainant may not be published even after the conclusion of an investigation, or may be published only on terms determined by the Authority.****”***