AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION

AUSTRALIAN CRIMINAL INTELLIGENCE MANAGEMENT STRATEGY 2017–20

INTELLIGENCE PARTNERSHIPS FOR A SAFER AUSTRALIA

Attorney-General's Department
Australia New Zealand Policing Advisory Agency
Australian Criminal Intelligence Commission
Australian Federal Police
ACT Policing
Australian Securities and Investments Commission
Australian Security Intelligence Organisation
Australian Taxation Office
Australian Transaction Reports and Analysis Centre
Department of Immigration and Border Protection/Australian Border Force
New South Wales Police Force
New Zealand Police
Northern Territory Police
Queensland Police Service
South Australia Police
Tasmania Police
Victoria Police
Western Australia Police

CONTENTS

FOREWORD

The United Nations Office on Drugs and Crime (UNODC) describes criminal intelligence as "*... the lifeblood of the fight against transnational organized crime. It is the foundation for all proactive investigations and a cross- cutting issue since the same expertise and methodology is used for all serious crimes, including, corruption, drug trafficking, and terrorism. A fundamental component of building law enforcement capacity involves enhancing understanding of how criminal intelligence works and how practically to develop, share and use it.*"[1]

The Australian Criminal Intelligence Model (ACIM) and associated Management Strategy (the Strategy) defines criminal intelligence as insights and understanding obtained through analysis of available information and data on complex offending patterns, serious organised crime groups, networks or syndicates and individuals involved in various types of criminal activities.

The Australian intelligence landscape is comprised of state, territory and federal law enforcement agencies (including policy and regulatory agencies) that operate within and across three separate but intersecting domains—national security, serious and organised crime[2], and policing and community safety. Criminal intelligence links all three domains and underpins our ability to understand these complex criminal environments and to identify threats, determine priorities and develop preventative response strategies.
As a community we are committed to improving our capacity to prevent and disrupt all crime types through a strong focus on intelligence capabilities and cooperative relationships.

Our state, territory and federal governments have overlapping responsibilities with respect to how we respond to criminal intelligence at local and national levels. In delivering this response, all jurisdictions and the Commonwealth are dedicated to nationally consistent methodology for the management of criminal intelligence. The ACIM and Strategy provide an agreed set of common standards, best practices and information sharing protocols for management of criminal intelligence assets. As Ministers and agency heads have different priorities the specific approaches adopted by individual agencies will reflect local circumstances but will align to the ACIM.

A central theme of the ACIM and Strategy is the notion of criminal intelligence being regarded as a national asset. The ACIM and Strategy provide a framework to harness and share our intelligence assets and support a whole of enterprise approach to capability management. Success of the Strategy is reliant on our ability to provide a collaborative and accountable culture for intelligence sharing with the appropriate underpinning technology, supportive policy and legislative frameworks. The Strategy mission, strategic objectives and underpinning principles guide us towards achieving our vision of ***intelligence partnerships for a safer Australia***.

1 Quoted from http://www.unodc.org/unodc.org/unodc/en/organised-crime/law-enforcement.html.
2 The serious and organised crime domain includes law enforcement, law compliance, policy and regulatory agencies.

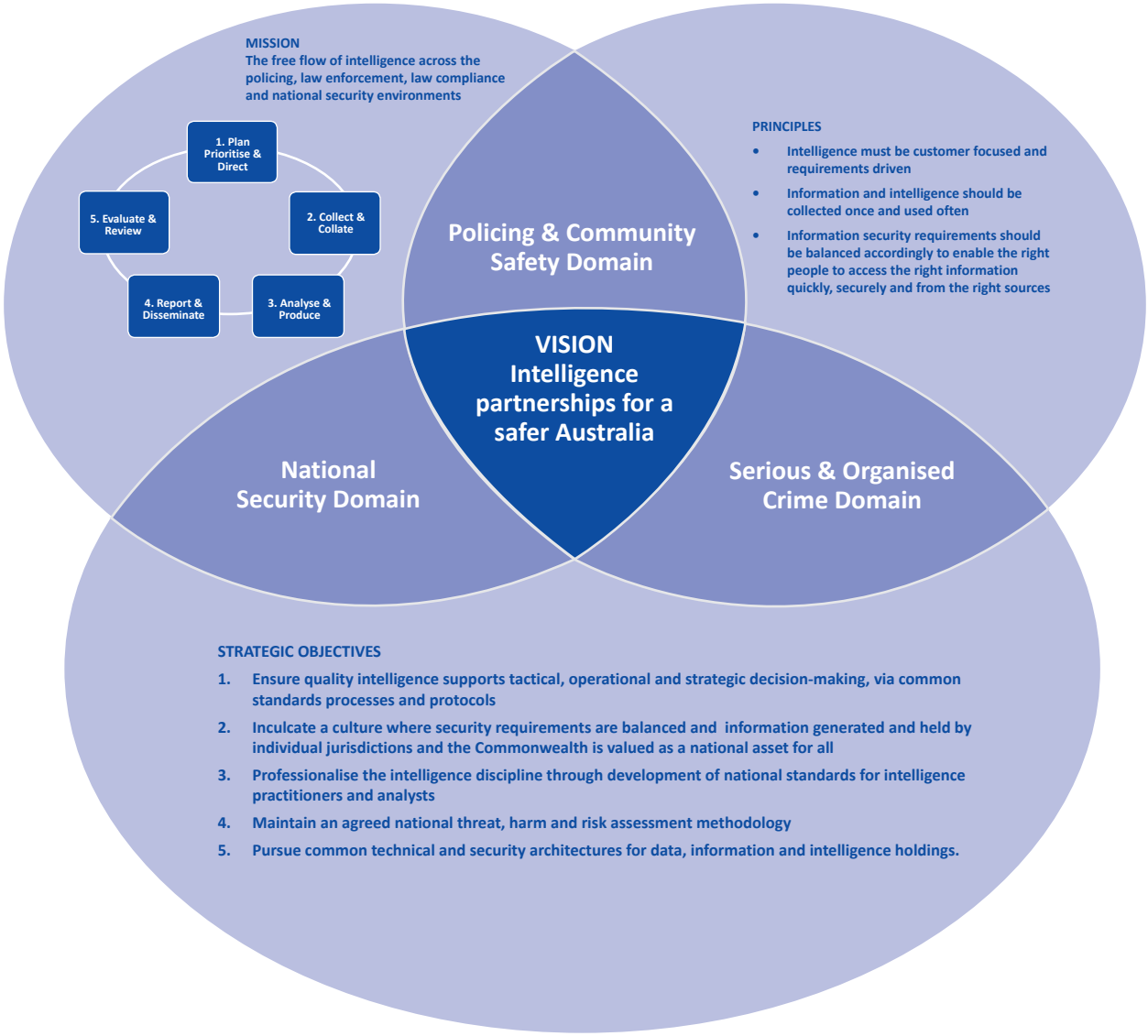
AUSTRALIAN CRIMINAL INTELLIGENCE LANDSCAPE

An accurate picture of criminality in Australia is dependant upon decision makers at all levels understanding the importance of sharing intelligence to assist in identification of threats, vulnerabilities and priorities. This intelligence serves as a decision advantage. The Australian intelligence landscape is comprised of multiple entities operating within and across various domains. We can gain national efficiencies by focusing on 'touch points' and partnerships to facilitate our mission of the free flow of intelligence across and between the operating domains. We can use technology, culture, policy and legislative initiatives to empower information sharing at and around the intersect points. By developing these enablers, the ACIM and associated Strategy will deliver a standard framework, through management of the intelligence cycle. Common functional themes, strategy initiatives and strategic objectives strengthen and enhance the criminal intelligence capabilities at all levels of law enforcement (including policy and regulatory agencies) in Australia.

The Strategy will facilitate accomplishment of this by using:

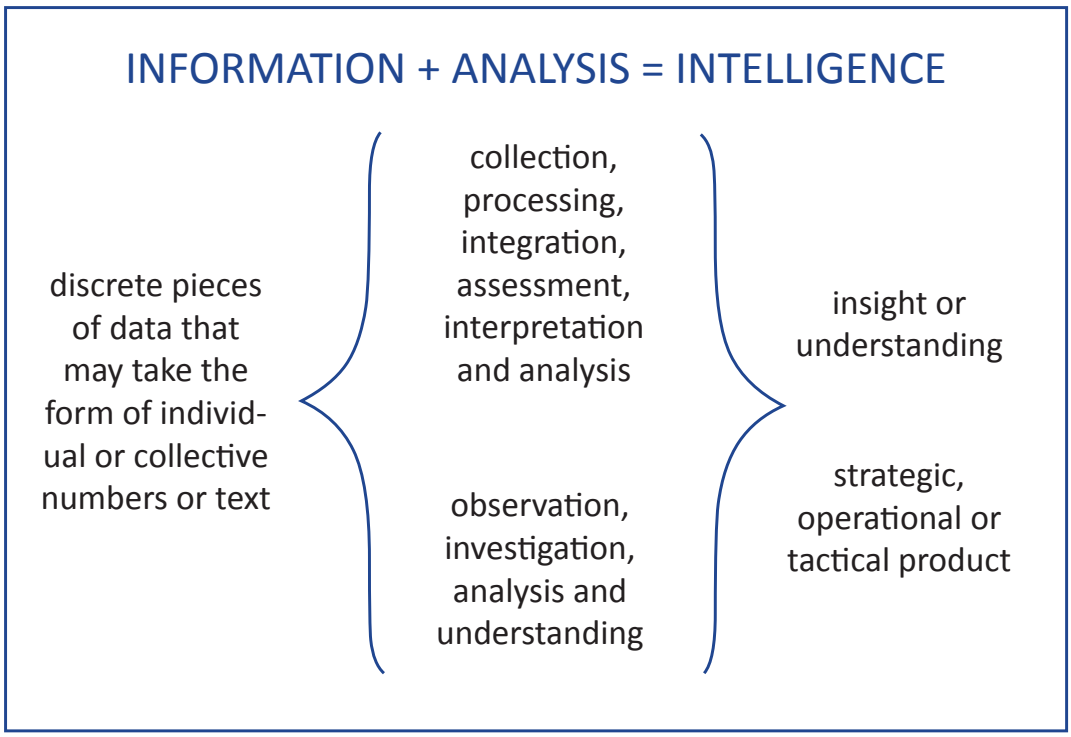
- technology to facilitate information sharing through interoperability of systems
- policy and legislation to underpin effective powers and processes for agencies to quickly and effectively collect, analyse and share relevant intelligence, and
- cultural norms to instil a collaborative attitude which ensures sharing is business-as-usual.

AUSTRALIAN CRIMINAL INTELLIGENCE MODEL



DEFINITION OF INTELLIGENCE

Intelligence takes the form of both an output and a process. The intelligence cycle is the process while products, insights and understanding are the output.



As a process, intelligence involves the collection, processing, integration, evaluation, interpretation and analysis of available information. This process typically referred to as the intelligence cycle transforms information into insight or understanding using analysis, critical thinking and problem solving skills. When different types of allied information are synthesised in this way they act as important building blocks in the intelligence process and are a critical precursor to an information or intelligence output. As an output, intelligence is the insights and understanding which are developed into a product for dissemination to support the different levels of decision-making, which can be strategic, operational or tactical. Another example of an output is criminal intelligence which is insights and understanding obtained through use of the intelligence cycle to analyse available information and data on complex offending patterns, serious organised crime groups or syndicates and individuals involved in various types of criminal activities.

OVERSIGHT AND IMPLEMENTATION

The National Criminal Intelligence Capability Committee (NCICC) is responsible for oversight and implementation of the ACIM and Strategy.

The NCICC was established as a part of the Australian Criminal Intelligence Commission's (ACIC) External Governance and Engagement Model (the Model). The Model establishes national committees with responsibility for technology, intelligence and operations. The NCICC is the intelligence capability committee.

The committee structure under which the NCICC operates provides opportunities for intelligence, operational and technical capabilities to work in collaboration to understand and respond to current and emerging crime threats, including by connecting police and law enforcement to the essential policing knowledge, intelligence and information they require.

The purpose of the NCICC is to promote and champion the professionalisation of the national criminal intelligence capability and to collaborate on strategic intelligence issues at a national level ensuring the coordination of advice for Australia's police, wider law enforcement and national security agencies.

Key responsibilities of the NCICC include:

- engagement with the ACIC and other relevant stakeholders to provide strategic advice to the ACIC CEO and Board relating to national criminal intelligence priorities and initiatives
- informing the development of national criminal intelligence priorities for Board consideration and endorsement
- leading the professionalisation of the criminal intelligence practice, including:
  - promoting common standards, processes and protocols for managing national intelligence
  - driving the analytical component for the National Criminal Intelligence System (NCIS)
  - overseeing the implementation of the ACIM and Strategy
  - developing a proposal for nationally consistent training for Intelligence practitioners
  - developing an Intelligence doctrine (value statement) to distinguish between intelligence practitioners and other specialist and experts, and
  - establishing focused intelligence capability sub-committees for topical issues and for specialised covert intelligence capabilities.
- informing the ACIC and other jurisdictions on:
  - intelligence-related information sharing services and/or systems, and
  - proposed changes to processes, policy direction and/or technology which may have a significant impact on national intelligence-related information sharing services and systems.

Consistent with their scope of responsibility and the strategic priorities of the ACIC, the NCICC may also be required to progress other specific activities as directed by the ACIC Board.

Membership:
Australian Criminal Intelligence Commission (ACIC), ACT Policing (ACTPol), Australian Border Force (ABF), Australian Federal Police (AFP), Australian Securities and Investments Commission (ASIC), Australian Security Intelligence Organisation (ASIO), Australian Taxation Office (ATO), New South Wales Police Force (NSWPF), Northern Territory Police (NTPol), Queensland Police Service (QPS), South Australia Police (SAPol), Tasmania Police (TasPol), Victoria Police (VicPol), Western Australia Police (WAPol).

Observer agencies: Australia New Zealand Policing Advisory Agency (ANZPAA), New Zealand Police (NZPol), Department of Immigration and Border Protection (DIBP), Australian Transaction Reports and Analysis Centre (AUSTRAC).

WHAT WILL SUCCESS LOOK LIKE?

Indicators of successful implementation of the ACIM will include:

- intelligence valued as a critical national asset
- more efficient use of limited resources and better risk management practices
- alignment of common standards, shared definitions, shared training, agreed competencies, and agreed curriculum for intelligence practitioners
- established best practice doctrine with emphasis on consistency in guiding principles and a program of continuous improvement
- policy and legislation to underpin effective national dissemination and Requests for Information (RFI) processes, and
- contemporary technology to enable more effective collection, analysis, storage and sharing of national intelligence assets.

HOW WILL WE ACHIEVE SUCCESS?

VISION

Intelligence partnerships for a safer Australia.

MISSION

The free flow of intelligence across the policing, law enforcement, law compliance and national security environments.

STRATEGIC OBJECTIVES

1. Ensure quality intelligence supports tactical, operational and strategic desision-making via common standards, processes and protocols.
2. Inculcate a culture where security requirements are balanced and information generated and held by individual jurisdictions and the Commonwealth is valued as a national asset for all.
3. Professionalise the intelligence discipline through development of national standards for intelligence practitioners and analysts.
4. Maintain an agreed national threat, harm and risk-assessment methodology.
5. Pursue common technical and security architectures for data, information and intelligence holdings.

CRITICAL SUCCESS FACTORS

- Policy and legislative framework to facilitate information sharing.
- Improved technical capabilities.
- A culture of national intelligence sharing.

Strategic Objectives

Each of the strategic objectives is underpinned by a series of action items to improve the efficiency and effectiveness with which we collect, collate, analyse, produce, store, disseminate, collaborate and share intelligence. Applying the strategies with an overarching approach will support better interoperability, consistency across domains and provide agencies with the flexibility to vary their priorities to suit local circumstances. The aim of the strategic objectives is to embed the ACIM through initiatives that increase the value-add of our intelligence for whole of enterprise decision-making.

Strategic Objective 1—Ensure quality intelligence supports tactical, operational and strategic decision-making via common standards, processes and protocols

1.1 Utilise working groups to leverage partnerships to guarantee there is timely exchange of the right information to the right people

1.2 Incorporate mechanisms for identifying regional and national priorities within agency/member collection plans

1.3 Promote standards and competencies for a nationally consistent language and approach for intelligence analysis

1.4 Initiate common processes and procedures to capture and share lessons learned and to support evaluation and review throughout the intelligence process, including metrics for assessing value-add of output

1.5 Ensure mechanisms are in place to share strategic, operational and tactical intelligence, nationally to support disruption and prevention activities

1.6 Improve linkages between agencies Request for Information (RFI) and dissemination processes to streamline requests and minimise duplication of effort

1.7 Facilitate timely dissemination of intelligence products by addressing (where possible) legislative and policy barriers to ensure data, information and intelligence is discoverable.

Strategic Objective 2—Inculcate a culture where security requirements are balanced and information generated and held by individual jurisdictions and the Commonwealth is valued as a national asset for all

2.1 Expand partnerships, where appropriate, to enhance opportunities for sharing (public sector, private enterprise), including through deployment of shared technologies.

Strategic Objective 3—Professionalise the intelligence discipline through development of national standards for intelligence practitioners and analysts

3.1 Build intelligence analyst tradecraft through development of national training standards and competencies

3.2 Develop a skilled and professional intelligence workforce with enhanced and shared professional development opportunities

3.3 Cultivate relevant experience and promote cross-jurisdictional peer review and mentoring to broaden experiences.

Strategic Objective 4—Maintain an agreed national threat, harm and risk assessment methodology

4.1 Ensure mechanisms are in place to facilitate access to the Threat Risk Assessment Methodology (TRAM) and to review and evaluate continued relevance of the TRAM for priorities across all domains.

Strategic Objective 5—Pursue common technical and security architectures for data, information and intelligence holdings

5.1 Deliver information sharing platforms and interoperable networks to:

- integrate existing cyber technologies to improve and expand knowledge of online functionality
- share analytical capabilities and exploit federated technologies to strengthen our ability to collect, collate and share intelligence by harnessing existing and new technologies, and
- align security architectures to streamline information and intelligence sharing across agencies and domains.

5.2 Identify common technical and security architecture solutions that can accommodate legal and policy requirements while ensuring data, information and intelligence is discoverable to those who require it.

CRITICAL SUCCESS FACTORS

The key to the success of the ACIM and Strategy will be in our collective ability to provide:

- the underpinning technology to facilitate information sharing through interoperability of systems
- the supporting policy and legislative framework including effective powers and processes for agencies to quickly and effectively collect, analyse and share relevant intelligence, and
- the collaborative culture of intelligence sharing to support decision making across operating domains.

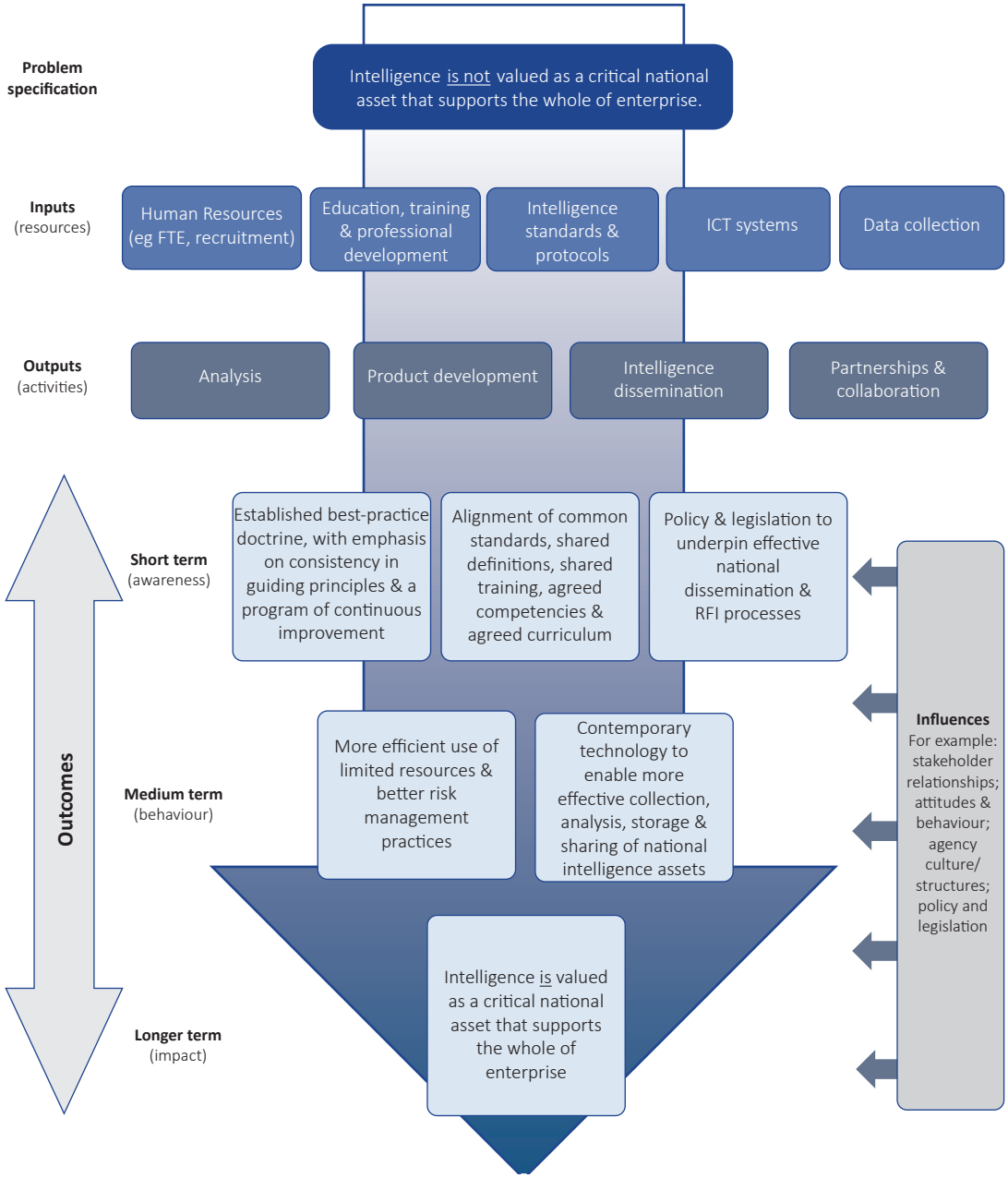
HOW WILL WE MEASURE SUCCESS?

For the success of the ACIM and Strategy to be accurately measured there needs to be a gauge of the value being created and a way to keep track of progress against the objectives. The gauges being used to measure success is a hybrid of a program logic and maturity model.

The program logic component is illustrated in the diagram which identifies the intended causal relationships between a program's inputs and its activities, and helps to determine if/how these achieve the program goals/outcomes while the table details characteristics of increasingly more 'mature' levels of the function across key domains.

The problem statement and associated inputs can be tailored to the particular issue being evaluated. The following diagram and table are targeted to demonstrate the success of the ACIM by measuring the goal of *intelligence valued as a critical national asset that supports the whole-of-enterprise.* The evaluation model demonstrates what needs to be achieved in terms of outcomes for the ACIM to be considered successful and the maturity model illustrates the various different levels of maturity of the process.

EVALUATION MODEL



MATURITY MODEL

	Awareness	Acceptance
Human Resources	• No recruitment framework • Analyst skills / knowledge not matched to position • Unclear link between staffing and intelligence objectives	• Clear role descriptions used consistently for intelligence analysts • Established approach to matching intelligence full time employees (FTE) with return on investment (ROI)
Education, Training and professional development	• Absent or online corporate training (only) • Inconsistent attendance at corporate training • Failure to understand performance development needs of the intelligence cohort	• Training is minimal and or not consistently completed • Training requirements are not linked to role suitability • Need for professional development noted inconsistently and opportunities for professional development are limited
Intelligence standards, protocols and processes	• Absent or inconsistent intelligence standards • Lack of agreed intelligence product suite • Limited relationship between intelligence focus & corporate objectives	• Corporate product suite exists but not used consistently • Basic processes established (eg RFI, dissemination) • Pockets of agreement on other standards & processes
Data collection	• Absence of an agreed corporate collection strategy • Ad-hoc approach, not linked to corporate or whole of government priorities	• Collection plan is clear and relates to current corporate priorities • Collection against these priorities is undertaken • Agency staff understand their collection responsibilities
Information Communication Technology (ICT) Systems	• System design fails to meet user needs • Lack of system integration • Systems fail to meet corporate and or security needs	• ICT policy is in place • ICT is available and reliable • Security protocols and processes in place

Defined	Managed	Excellence
• Established multi-level career paths(s) for intelligence staff • Investment in developing intelligence leaders and mentors	• Tailored learning and development processes to support specialist intelligence streams • Corporate approach to balancing specialisation versus flexibility	• Consistent use of robust recruitment practices • Clear link between resourcing and corporate outcomes.
• Robust training at multiple levels is required for all intelligence roles • Training needs analysis and best practice underpin further developments • Experienced intelligence professionals identified as capability leaders.	• Analysts take responsibility to develop professionally (facilitated by managers) • Training and professional development focus and approach simultaneously meets individual, team and organisational goals	• Development program underpinned by detailed role descriptions and performance evaluations • Continuous improvements ethos approach to intelligence capability.
• Corporate documentation of intelligence processes, terminology, methodologies etc • Consistent application of these (including peer review) is business as usual • Intelligence activities are client-focused	• Intelligence standards, protocols & processes are integrated with other corporate functions • Includes an agreed corporate approach to intelligence evaluation • Strong client relationships support regular feedback	• Organisational structure reflects the purpose of the intelligence function • Clients proactively seek intelligence input critical to decisions • Executive leadership of the intelligence function
• Collection plan includes current required activity and anticipates future collection needs (e.g. meets strategic requirements) • Collection is undertaken across a range of agency units and divisions • Engagement of key stakeholder in strategy development	• Clear and detailed instructions for data collection activity • Collection draws on diverse data and information sources and is well resourced • De-confliction activity to mitigate collection duplication	• Data collection strategy aligns with corporate and whole of government priorities • Collection strategy defines agency collection requirements according to current and future priority levels, risks and gaps • Collection activity is actively driven across all elements of the plan
• System users are involved in system design • Systems have partial integration • Information policy clearly articulates access, privacy, intellectual property and archiving requirements • ICT policy and planning is typically focused on current requirements	• ICT is responsive to corporate requirements • Systems are largely integrated and can manage divers data types • Master ICT plan is in place that articulates further needs	• Systems are flexible and fully integrated across different functional areas • Systems meet International Organisation for Standardisation (ISO) requirements • Forward planning clearly articulated and focused on continuous improvement • ICT meets whole of organisational needs.

CONCLUSION

The ACIM and Strategy support management of criminal intelligence more holistically through collaborative use of best practices, standards, competencies, technologies, policies and legislative initiatives to empower information sharing through committees and forums that facilitate enhancement of criminal intelligence capabilities at all levels of law enforcement (including policy and regulatory agencies) in Australia. Implementation of the ACIM and Strategy will create the framework for improved intelligence coordination and will further facilitate development of innovative national information and intelligence sharing services between state, territory and federal law enforcement agencies. This will unite partners to achieve outcomes that cannot be achieved individually through improved national intelligence responses, improved intelligence capabilities and strengthened partnerships for a safer Australia.

REFERENCES

Australian Criminal Intelligence Management Strategy 2012–15
http://www.unodc.org/unodc.org/unodc/en/organised-crime/law-enforcement.html