Victoria Police response to IBAC’s Operation Genoa

Victoria Police responded in December 2018 regarding the development of a more robust information security framework.

IBAC publishes responses to our investigations to inform the community about actions agencies advise they are taking, and to share learnings that may help other agencies improve their systems and practices to prevent corruption and misconduct.

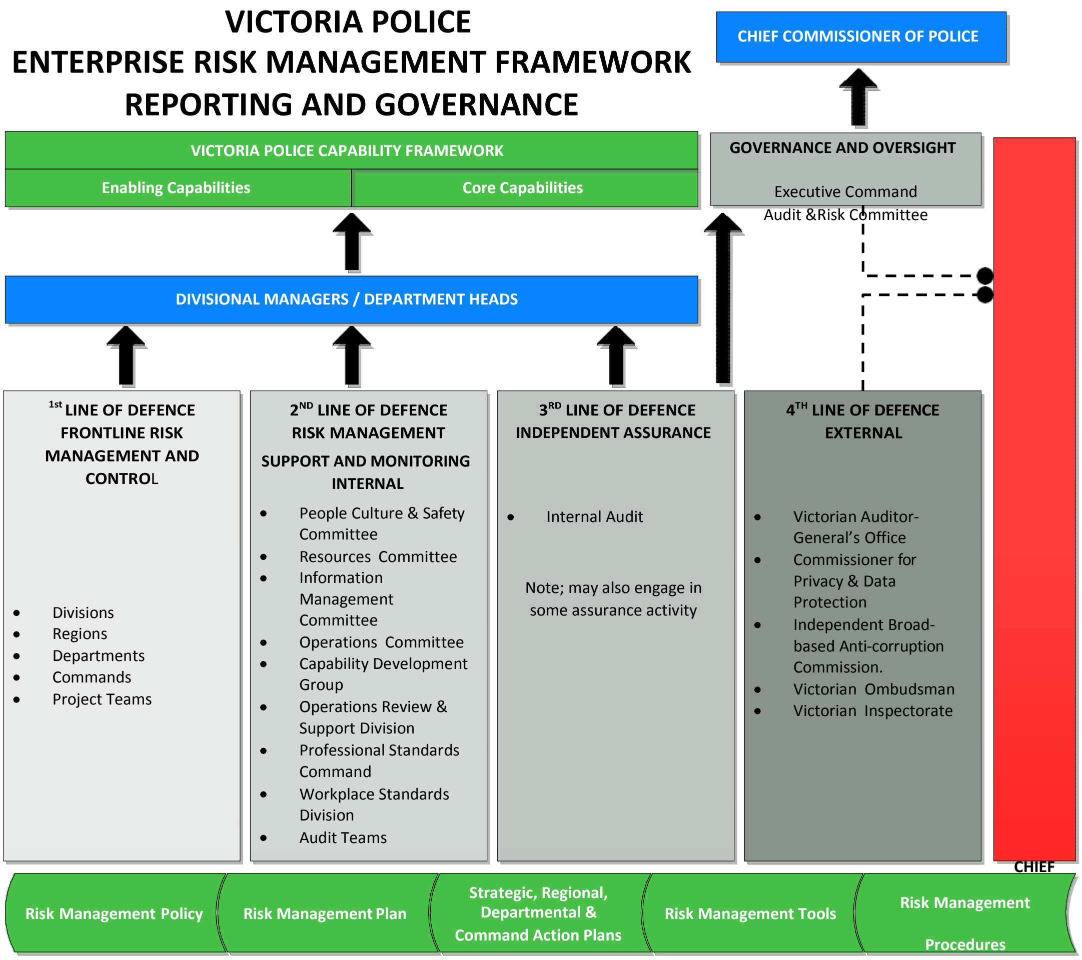
Victoria Police’s response is as follows:

Review of procedures for preventing and detecting information misuse

The Victoria Police Enterprise Risk Management Framework (ERMF) describes the arrangements operating within the organisation to manage its organisational risks, including the risks to law enforcement information through misuse. Under the ERMF the four lines of defence model attribute responsibilities for risk management as follows:

1. Frontline risk management and control
2. Support and monitoring internal
3. Independent assurance
4. External

Figure 1: Victoria Police Enterprise Risk Management Framework


VICTORIA POLICE
ENTERPRISE RISK MANAGEMENT FRAMEWORK
REPORTING AND GOVERNANCE
CHIEF COMMISSIONER OF POLICE
VICTORIA POLICE CAPABILITY FRAMEWORK
Enabling Capabilities
Core Capabilities
GOVERNANCE AND OVERSIGHT
Executive Command
Audit &Risk Committee
DIVISIONAL MANAGERS / DEPARTMENT HEADS
1st LINE OF DEFENCE FRONTLINE RISK MANAGEMENT AND CONTROL
Divisions
Regions
Departments
Commands
Project Teams
2ND LINE OF DEFENCE RISK MANAGEMENT
SUPPORT AND MONITORING INTERNAL
People Culture & Safety Committee
Resources Committee
Information Management Committee
Operations Committee
Capability Development Group
Operations Review & Support Division
Professional Standards Command
Workplace Standards Division
Audit Teams
3RD LINE OF DEFENCE INDEPENDENT ASSURANCE
Internal Audit
Note; may also engage in some assurance activity
4TH LINE OF DEFENCE EXTERNAL
Victorian Auditor-General’s Office
Commissioner for Privacy & Data Protection
Independent Broad-based Anti-corruption Commission.
Victorian Ombudsman
Victorian Inspectorate
CHIEF
Risk Management Policy
Risk Management Plan
Strategic, Regional, Departmental & Command Action Plans
Risk Management Tools
Risk Management Procedures

Under the model, the Information, Systems & Security Command (ISSC) operates at the 2nd line of defence to provide policy and guidance relating to information management and information security to the organisation operating at the 1st line of defence. ISSC ensures that regulatory standards from the Office of the Victorian Information Commissioner (OVIC) and the Public Record office of Victoria (PROV) are addressed through Victoria Police policy in the Victoria Police Manual.

ISSC is also responsible for providing Information Communication Technology (ICT) to the organisation that not only meets operational needs but which addresses threats to law enforcement information.

ISSC also provides security incident reporting and response services to the organisation.

The Professional Standards Command (PSC) operates at the 2nd line of defence to enhance and promote a culture of high ethical standards throughout the organisation. The focus for PSC is on effective prevention, deterrence and investigation of corrupt behaviour, criminality and misconduct.

The Risk and Assurance Division (RAD) under the Strategic Investment, Reporting and Audit (SIRA) Department operates at the 3rd line of defence to provide internal auditing services. Besides a rolling program of targeted audits scheduled through the Victoria Police Audit and Risk Committee (ARC), RAD operates a program of continuous audits focusing on the ongoing assessment of key controls to provide reasonable assurance that they are adequate and effective.

Victoria Police concurs with the advice from IBAC that there are often strong correlations between ethical health and information misuse, and as a result ISSC has liaised with RAD and PSC to review current processes and future intentions for preventing and detecting information misuse.

ISSC created the Information Management & Information Security (IM&IS) policy framework within the Victoria Police Manual to instruct members on how to classify and handle information appropriately as well as the ICT solutions used to process Victoria Police information. Between 2013 and 2016 ISSC ran a cultural change program to address information security risks identified during an organisational review in 2011, performed in conjunction with the Victorian Managed Information Authority (VMIA). Subsequently ISSC created the IM&IS portfolio holders' network to disseminate information and guidance across the organisation.

ISSC also liaises closely with Legal Services and Procurement to ensure that IM&IS requirements are embedded into formal arrangements such as contracts, Memorandums of Understanding (MOUs) and Letters of Agreement (LOAs) etc., to address information sharing risks. ISSC's ICT systems auditing team manages the auditing provisions of the agreements with Authorised Third Parties that are provided with access to Victoria Police ICT systems as well as an audit facilitation service for RAD and PSC.

In 2016, ISSC secured funding for a program of cyber security controls uplift under the BlueConnect program to address the growing threats to Victoria Police's information and ICT systems. The program identified a variety of technical and governance controls for improvement as well as funding three new roles, two of which are dedicated to ICT systems auditing.

At around the same time the newly formed OVIC issued the Victorian Protective Data Security Standards (VPDSS). In July 2017 OVIC rescinded the compliance obligations for Victoria Police with the previous Standards for Law Enforcement Data Security (SLEDS) and replaced them with an obligation to comply with the VPDSS.

As part of the VPDSS compliance activities ISSC undertook a Security Risk Profile Assessment (SRPA) to assess risks to Victoria Police's information assets, a self-assessment against the VPDSS controls and developed a Protective Data Security Plan (PDSP). The PDSP and accompanying attestation were supplied to OVIC and acceptance of compliance was received in return.

In 2018 Victoria Police developed its Cyber Security Strategy in response to the Victorian Government's Cyber Security Strategy (2017) and to align activities across ISSC to address the Organisational Risks of cyber intrusion and information misuse.

ISSC is using the PDSP and Cyber Security Strategy to strengthen preventative and detective controls for information misuse.

RAD maintains the Enterprise Risk Management Framework (ERMF) and an auditing capability that assesses the efficacy of organisational processes. SIRA is in the process of revising the ERMF to be in line with the Capability Framework to ensure risks across the 30 core and 48 enabling capabilities are identified and managed appropriately. One of the five fundamental inputs to capability is technology which includes both information and ICT systems.

The Continuous Auditing Team within RAD operates a program of ICT systems audit to ensure access controls are effectively managed. For example, ensure user access is removed in a timely manner when no longer required. The audit program also targets user activities to ensure controls are in place to prevent inappropriate usage of critical ICT systems.

In 2016, PSC implemented the Ethical Health Assessment Process (EHAP) focusing on staff behaviours. The EHAP is an early intervention model that is supported via an automated alert system which is initiated:

- when an employee attracts three complaints within a 12-month period within the Victoria Police Register of Complaints Serious Incidents and Discipline (ROCSID) and/or through daily proactive (manual) monitoring conducted by PSC Intelligence Practitioners;
- where a single event is assessed as sufficiently significant to warrant the assessment or at the request of an employee's manager whose engagement with an employee indicates that the person's behaviour is an emerging issue and risk.

The EHAP then causes an analysis of a number of data sources including operational and human resource systems to be undertaken. Where the EHAP identifies a change in behaviour or an emerging issue that indicates an ethical and/or welfare risk to the employee, an Employee Ethical Assessment Profile (Profile) is generated for dissemination and consideration by the employee's Divisional Superintendent and the local Ethical and Professional Standards Officer (EPSO). The intent of this notification is to prompt an intervention with the employee.

PSC has engaged with several external providers, in particular Monash and Deakin Universities, in an effort to design and implement an automated data science platform that will assist in the early identification of employees at higher risk of being involved in an adverse event without some form of early intervention. A pilot of the platform has been formally proposed and approved and project activities are in the process of commencing.

The changes proposed to the Victoria Police complaint handling model will compliment these proactive processes, by placing greater responsibility on managers to performance manage employees. The changes seek to utilise the Performance Development Assessment (PDA) application so that managers are able to handle performance issues relating to their employees, including creating management plans and using development opportunities to improve behaviour.

Strengthened liaison between ISSC, RAD and PSC is planned as the programs outlined above are rolled out to ensure the processes to address information misuse are appropriate for the risks, gaps are addressed and overlap is minimised for efficiency.

Victoria Police submits that this recommendation is acquitted.

Strengthen audits of information systems (particularly LEAP, Neo and Interpose)

ISSC deployed a proactive auditing capability as part of the BlueConnect cyber security uplift project to address activities outlined in ISSC's Protective Data Security Plan.

One of the primary drivers for the program of work is a number of recommendations originating from the following audit reports:

- User Access Application / Review of Key Systems (2016)
- Victoria Police Information Access Arrangements: A Critical Analysis (2012)
- Interpose Logging and Audit Review (2011)
- Review of Victoria Police Compliance with CLEDS Standards on Access Control and Release of Law Enforcement Data (2008)

A roadmap and implementation plan were developed in conjunction with RAD and PSC. It has commenced implementation with several critical applications and includes a feedback cycle to ensure activities continue to be aligned to organisational goals and risks through liaison with RAD and PSC and tracking of identified security incidents. These will be cross referenced with other incident notifications received through other information sources.

The BlueConnect project team has also devised a benefits realisation plan for the cyber security uplift project which includes the organisational benefits of the proactive auditing capability. This will provide a separate layer of governance that will help the team achieve their goals.

Victoria Police submits this recommendation has been acquitted.

Consult with the Office of the Victorian Information Commissioner on the adequacy of these procedures and audits in line with the Privacy and Data Protection Act 2014

Victoria Police liaises on a regular basis with OVIC both in relation to the fulfilment of audit recommendations and the management of information security risks.

The Chief Information Officer, head of ISSC, and the Director of Security & Management Services within ISSC are the designated contact points for liaison with OVIC, the Deputy Commissioner for Privacy & Data Protection and relevant staff.

OVIC has received and approved Victoria Police's Protective Data Security Plan to address information security risks.

The roadmap for the proactive auditing capability includes OVIC recommendations relating to ICT systems audit and as the recommendations are met the new security controls will be officially communicated to OVIC for acceptance and closure.

Victoria Police submits this recommendation is acquitted.