



NEW SOUTH WALES AUDITOR-GENERAL'S REPORT

Upgrades to core policing technology

PERFORMANCE AUDIT | 11 MAY 2026

THE ROLE OF THE AUDITOR-GENERAL

The roles and responsibilities of the Auditor-General and the Audit Office, are set out in the *Government Sector Audit Act 1983* and the *Local Government Act 1993*.

We conduct financial or 'attest' audits of state public sector and local government entities' financial statements. We also audit the Consolidated State Financial Statements, a consolidation of all state public sector agencies' financial statements.

Financial audits are designed to give reasonable assurance that financial statements are true and fair, enhancing their value to end users. Also, the existence of such audits provides a constant stimulus to entities to ensure sound financial management.

Following a financial audit the Audit Office issues a variety of reports to entities and reports periodically to Parliament. In combination, these reports give opinions on the truth and fairness of financial statements, and comment on entity internal controls and governance, and compliance with certain laws, regulations and government directives. They may comment on financial prudence, probity and waste, and recommend operational improvements.

We also conduct performance audits. These assess whether the activities of government entities are being carried out effectively, economically, efficiently and in compliance with relevant laws. Audits may cover all or parts of an entity's operations, or consider particular issues across a number of entities. Our performance audits may also extend to activities of non-government entities that receive money or resources, whether directly or indirectly, from or on behalf of government entities for a particular purpose.

As well as financial and performance audits, the Auditor-General carries out special reviews, compliance engagements and audits requested under section 27B(3) of the *Government Sector Audit Act 1983*, and section 421E of the *Local Government Act 1993*.



GPO Box 12
Sydney NSW 2001

The Legislative Assembly
Parliament House
Sydney NSW 2000

The Legislative Council
Parliament House
Sydney NSW 2000

In accordance with section 38EC of the *Government Sector Audit Act 1983*, I present a report titled '**Upgrades to core policing technology**'.

A handwritten signature in black ink, appearing to read 'Bola Oyetunji'.

Bola Oyetunji

Auditor-General for New South Wales
11 May 2026

RECONCILIATION STATEMENT

We pay our respect and recognise Aboriginal peoples as the traditional custodians of the land in NSW who have cared for and protected the environment, waterways, and sacred sites over many millennia. We honour and thank the traditional custodians of the land on which our office is located, the Gadigal people of the Eora Nation, and the traditional custodians of all the lands on which our employees live and work. We pay our respects to their Elders past and present, and to the next generation of leaders.

We also acknowledge that our long history is shared with the histories of colonisation in New South Wales. We acknowledge the impacts of colonisation, and the resulting marginalisation and disadvantage of Aboriginal and Torres Strait Islander peoples in this state.

We embrace our role in holding government agencies to account for the delivery of effective services for Aboriginal and Torres Strait Islander peoples. We are committed to ensuring that our audits are culturally responsive, respectful and inclusive, and that we engage with Aboriginal and Torres Strait Islander peoples and communities in a meaningful and collaborative way.

We recognise the ancestral tie of Aboriginal and Torres Strait Islander peoples to this land, and we acknowledge that we have much to learn from their wisdom, rich and diverse culture, languages, knowledge and practices.

contents

Upgrades to core policing technology

1.	Report snapshot	1
2.	Executive summary	2
	Conclusion	2
3.	Introduction	6
	3.1. Overview of the NSW Police Force	6
	3.2. ICT and procurement frameworks	6
	3.3. Core policing technology systems	7
4.	Initial business case and procurement	10
5.	Transitional delivery	16
6.	Program reset	20
	Appendix 1 – Response from entity	28
	Appendix 2 – Timeline of key events	34
	Appendix 3 – Gateway reviews and health checks	35
	Appendix 4 – Status of PTP projects at December 2025	38
	Appendix 5 – About the audit	40
	Appendix 6 – Performance auditing	42

1. Report snapshot

Objective

This audit assessed whether the NSW Police Force efficiently and effectively planned and sourced key components to upgrade core policing technology systems.

Key findings

The NSW Police Force did not effectively plan and has not yet delivered the program

By December 2025, the NSW Police Force had spent over \$155 million delivering some essential technology upgrades and replacing only 1 of 5 core systems in full, with most functions still dependent on outdated platforms.

The contract was awarded to a supplier that posed a high delivery risk

The NSW Police Force conducted a structured and competitive procurement that complied with NSW Government requirements. However, despite warnings from advisers and gateway reviews, it proceeded with a supplier whose solution promised operational benefits even though it posed known capability and delivery risks.

Supplier non-performance caused delays and costs with no ongoing benefit

The selected supplier was unable to deliver key system components. The NSW Police Force terminated the contract in 2022 after significant delays and expenditure.

There was no effective oversight of timelines, budget controls or risks

Following contract termination, the NSW Police Force did not maintain effective governance, capability or appropriate financial controls. This slowed decision making and prolonged reliance on legacy systems.

The NSW Police Force reset the program in mid-2024, reducing program delivery risks

Since mid-2024, there have been significant improvements to governance and program management, and the NSW Police Force has developed an enterprise digital strategy. These have stabilised the program.

The NSW Police Force estimates it needs additional funding to deliver the program

The program delivery date is now June 2031, 4 years later than originally planned. The NSW Police Force estimates that it will need an additional \$78 million in capital funding and \$415 million in recurrent funding to deliver the program.

Recommendations

The NSW Police Force should demonstrate effective program governance throughout the remaining life of the program and incorporate lessons learnt to manage risks to ensure program success.

Fast facts

\$155m

amount of program capital budget allocated in 2021 spent by December 2025 (47%)

4 years

delay between original program completion date (2027) and forecast completion date (2031)

\$493m

NSW Police Force estimate of additional funding required to complete the program by 2031

2. Executive summary

Context

As of June 2025, the NSW Police Force, Australia's largest law enforcement agency, had nearly 16,000 sworn officers and 4,500 civilian staff serving almost 8.5 million people across 801,600 square kilometres. The NSW Police Force requires robust technology systems to give frontline officers timely information at incidents and to process crime records efficiently to support judicial process and improved community safety.

The Computerised Operational Policing System (COPS) is the NSW Police Force's primary system to support police operations. It was implemented in 1994 and is hosted on outdated mainframe technology, using an obsolete programming language. COPS supports day-to-day policing by recording incidents and maintaining information to support case management and investigative activity. Other core policing technology systems that support activities include computer aided dispatch (CAD), forensics and exhibits management, custody management, and major investigations and intelligence gathering. These systems are critical for effective policing in NSW.

The NSW Police Force has made several attempts to upgrade or replace its core systems since 2006. This audit focuses on the activities of the NSW Police Force to replace core systems from 2018 to 2025. The program to replace core policing systems was known as the Integrated Policing Operating System (IPOS) from 2018 until 2024, when it was renamed the Police Technology Program (PTP). The audit did not review administrative systems used for staffing, rostering or finance, or other technology and equipment used by frontline staff, such as body-worn video.

On 20 November 2024, the Law Enforcement Conduct Commission (LECC) referred a complaint to the Audit Office of New South Wales under section 162 of the *Law Enforcement Conduct Commission Act 2016*, concerning the NSW Police Force's administration of the IPOS project. The Auditor-General accepted this referral and began the audit in 2025.

Audit objective

This audit assessed whether the NSW Police Force has efficiently and effectively planned and sourced key components to upgrade technology systems that support core policing functions. The audit assessed this with the following questions:

1. Did the NSW Police Force effectively plan for upgrades to technology to support core policing functions?
2. Was the procurement of core policing technology systems transparent, competitive and compliant with NSW Government policies and procedures?
3. Did the NSW Police Force establish and maintain effective governance of core policing technology upgrades?

Conclusion

The NSW Police Force has not efficiently or effectively planned and sourced key components to upgrade core policing technology systems.

The NSW Police Force did not adequately plan critical system upgrades. Despite spending over \$155 million (47% of the \$328 million allocated program budget) between March 2021 and December 2025, several replacement systems are still outstanding. The NSW Police Force has upgraded essential supporting technology infrastructure and delivered 1 of the 5 core systems. The slow progress has required the NSW Police Force to allocate program funds to extend the life of its legacy systems. In the meantime, the delay in delivery has resulted in technology and operational risks and reduced operational effectiveness. The NSW Police Force has identified it has insufficient funding to deliver the program and will not complete it until 4 years later than originally planned.

The NSW Police Force conducted a structured and competitive procurement process in 2019, which included external assurance, to select suppliers for the program. In 2020, the NSW Police Force awarded the contract through a competitive process to a US technology firm whose product best met operational requirements. This was despite uncertainty about the supplier's capability. Ultimately, the supplier was unable to deliver, which resulted in lengthy delays to the program and waste of public resources.

The NSW Police Force did not establish and maintain effective governance to support timely and coordinated program delivery. However, following an external review of the program in 2024, both governance and program management have improved significantly.

Key findings

Operational, financial and technology risks identified in the 2018 strategic business case remain unaddressed due to program delays

For more than a decade, the NSW Police Force recognised that its core policing technology systems, particularly COPS, had reached or exceeded end of life. The strategic business case for the program prepared in 2018 documented operational, financial and technology risks arising from continued reliance on legacy systems, including reduced frontline efficiency, rising maintenance costs and difficulty recruiting staff with specialist skills. In the 2025 updated business case, the NSW Police Force noted escalating risks to service continuity, cyber security and public safety.

The NSW Police Force received funding for the program in February 2021, which included upgrades to technology infrastructure. By December 2025, the NSW Police Force had spent around \$155 million of the approved \$328 million capital allocation for the core technology program. Program delays and underspend occurred because the supplier selected by the NSW Police Force was unable to deliver the product in accordance with the contract.

While essential technology infrastructure and the forensics and exhibits system have been upgraded, other core systems identified in the original business case remain dependent on legacy platforms. This requires ongoing funding, increases technology risk and reduces operational effectiveness.

Despite a thorough procurement process, the NSW Police Force selected a supplier identified as high risk, and developed mitigation strategies to reduce contract risk

The NSW Police Force conducted a comprehensive and competitive procurement process for IPOS between 2018 and 2020. The process included extensive scenario testing, site visits, external probity advice and gateway reviews. It complied with NSW Government procurement requirements. The procurement process identified 3 viable suppliers to deliver the product.

The NSW Police Force selected an overseas start-up technology firm ahead of 2 other viable suppliers because the preferred supplier scored higher on operational criteria. It accepted risks associated with this supplier, supported by a series of contractual risk mitigation measures. Gateway reviews and external advisers had warned NSW Police Force decision makers about delivery optimism and the program's resourcing constraints. They also warned about capability risks for the highest ranked supplier. In addition, the NSW Police Force's legal and procurement advisers raised concerns about the preferred company's financial position, limited experience delivering systems of comparable scale, and the absence of key capabilities, such as forensics and exhibits.

In June 2022, the supplier advised the NSW Police Force that it could not deliver a forensics and exhibits system, and that delivery of a minimum viable CAD capability would be delayed by several years. The NSW Police Force terminated the contract when it became clear that the supplier could not meet contractual milestones. Up until then, the NSW Police Force had spent close to \$20 million in expenditure on work that delivered no ongoing benefit.

To reduce the likelihood of repeating this experience, the NSW Police Force has since changed its procurement approach, moving away from a single vendor delivery model and applying stricter requirements for supplier capability and experience.

The NSW Police Force has delivered several systems and upgraded essential information and communications technology infrastructure

Since funding was approved in 2021, the NSW Police Force has delivered or partially delivered several systems, including a replacement for the forensics and exhibits system. It has also made improvements to critical information and communications technology (ICT) infrastructure such as cloud hosting, security and systems integration. These investments support operational policing and enable capability for future core systems.

The NSW Police Force has delivered upgrades to mobile policing tools, including streamlining the recording of inspections and domestic violence incidents. It has also introduced a system that allows police to interact directly with the public through location sharing and live video.

The NSW Police Force went out to tender for a new CAD system in early 2024 and expects to deliver the upgrade in 2027. In late 2024 it re-started the procurement process for a replacement for COPS.

The NSW Police Force reset program governance and delivery arrangements in 2024, addressing weaknesses experienced earlier in the program, but key person reliance remains a risk

Between 2022 and 2024, the program steering committee did not provide consistent business leadership or effective oversight of timelines, budgets or risks. Internal audits, gateway reviews and external reviews during this period consistently highlighted weaknesses in program management, decision making and financial control.

At the same time, the NSW Police Force found it difficult to recruit and retain staff with specialist ICT and program management capability, including staff with legacy system knowledge required to maintain COPS while planning its replacement. These factors delayed the program.

In mid-2024, the NSW Police Force initiated a program reset. Senior leaders clarified accountability, strengthened governance structures and introduced more consistent project reporting and financial tracking. The NSW Police Force revised the program strategy and operating model, introduced a phased implementation approach and improved program assurance. The NSW Police Force has also developed a digital strategy that provides clarity to the program.

These changes have stabilised the program and improved decision-making transparency. Independent health check reviews conducted in 2024 and 2025 acknowledged improvements in governance and program management and assessed overall delivery confidence as medium, while noting the importance of ensuring continuity of key personnel. The program remains vulnerable to setbacks if the capability of key personnel is diminished.

Full delivery is not expected until 2031, 4 years after the originally identified end date

Critical components of the core technology program remain outstanding. In the 2020 final business case, the NSW Police Force had planned to upgrade core policing systems by June 2027. The 2024 program reset revised the program end date to 2031, 4 years later than originally planned. Phase 1 of the program is now scheduled for completion in 2029, with phase 2, including COPS modules for intelligence management and custody management, due in 2031.

In the meantime, the NSW Police Force has maintained end-of-life legacy systems for significantly longer than expected, increasing both capital and recurrent expenditure on systems that do not contribute to future capability. Continued reliance on legacy systems also exposes the NSW Police Force to technology risk and reduces operational effectiveness.

The NSW Police Force estimates it will require additional capital and recurrent funding to complete the program due to rising costs, a change in strategy and earlier incorrect assumptions

The NSW Police Force prepared a revised program business case in late 2025, which estimates it will require an additional \$78 million in capital funding (additional to the \$328 million allocated in 2020). It also estimates it will require \$415 million in recurrent funding to deliver the remaining program components from 2026 through to 2031.

The revised business case attributes the additional funding need to rising costs of ICT salaries, less favourable contract terms than it was able to secure in 2020, the move to a multi-vendor strategy and incorrect assumptions made in the 2020 business case. The NSW Police Force had previously expected that decommissioning the mainframe systems and moving to 'software-as-a-service' would reduce recurrent expenditure by around \$25 million per year from 2027–28 to 2038–39.

Recommendations

Throughout the remaining life of the program, the NSW Police Force should:

1. demonstrate effective program governance arrangements that:
 - a) support delivery of the Police Technology Program in line with planned milestones
 - b) maintain robust budget controls to align spending with approved funding and scope, and to ensure early identification and management of variances
 - c) achieve intended outcomes by driving clear accountability, effective oversight of delivery risks and assessment of value for money
 - d) ensure effective management of technology-enabled transformation and organisational change
 - e) ensure the required capability is maintained
2. apply lessons learned from the early procurement and program management experience to the program, particularly in relation to procurement capability, supplier selection and early intervention where delivery risks emerge.

3. Introduction

3.1. Overview of the NSW Police Force

The NSW Police Force is organised through a statewide command structure made up of metropolitan and regional police areas that are divided into local police area commands and police districts. Frontline policing is supported by specialist commands and central corporate functions that provide services across the organisation and support consistent operations across the state. The Technology and Communication Services Command provides information and communications technology (ICT), data, cyber security and communications services that support frontline policing, specialist operations and corporate functions across the NSW Police Force.

The organisation is led by the Commissioner of Police and governed through senior executive governance groups. The NSW Police Force has a mixed workforce made up of sworn police officers – in frontline policing and specialist law enforcement roles – and civilian staff who support these activities by providing corporate, professional and specialist services. In June 2025, the NSW Police Force comprised nearly 16,000 sworn officers and 4,500 civilian staff.

3.2. ICT and procurement frameworks

ICT strategies and frameworks

The NSW Police Force operates within a whole-of-government policy environment that sets expectations for digital investment, cyber security, and the protection of people, information and assets.

The NSW Digital Strategy sets out the NSW Government's approach to digital transformation, including improving service delivery, modernising legacy systems, and strengthening data and technology capabilities across government agencies. It emphasises user-centred design, systems that work well together, effective governance, and responsible use of data to support better outcomes and value for money.

The NSW Cyber Security Policy sets mandatory requirements for NSW Government agencies to manage cyber security risks. Agencies must implement appropriate governance, risk management and technical controls to protect information and systems from cyber threats, including risks from using legacy systems, integration between systems and working with third-party service providers.

At the Commonwealth level, the Australian Protective Security Policy Framework (PSPF) provides principles and minimum requirements for safeguarding government people, information and assets, both within Australia and internationally. It is the Australian Government's overarching framework for managing security risks, and covers 6 security domains, including personnel, information, technology and governance. The framework applies to NSW Government agencies that hold or access Australian Government security classified information.

NSW Government procurement standards and oversight

NSW Government agencies must follow whole-of-government procurement policies and frameworks when buying goods and services to ensure value for money and manage risks. For ICT procurements, agencies are expected to use the NSW Government ICT Purchasing Framework, which sets out approved procurement methods and contract arrangements.

NSW Treasury plays a central role in overseeing major government expenditure, including setting requirements for business cases and investment decisions for significant ICT projects. Treasury guidelines inform how agencies develop and seek approval for capital and recurrent funding and ensure proposals fit within government priorities and available budgets.

The NSW Department of Customer Service (DCS) has a key role in digital and ICT governance across the NSW public sector. The DCS administers the NSW ICT Digital Assurance Framework, which applies to major ICT projects and provides a risk-based, independent assurance process. The framework is intended to provide government decision makers with confidence that ICT initiatives are appropriately planned, governed and managed.

As part of this framework, gateway reviews are conducted at defined stages of major ICT projects, including during strategic planning, business case development and procurement. Gateway reviews provide independent assessments of project readiness, delivery confidence and key risks, and are used to inform decisions about whether projects should proceed to the next stage.

Between 2019 and 2025 there were 7 independent reviews of the NSW Police Force's core technology program plus one internal audit. These are described in Appendix 3.

3.3. Core policing technology systems

This audit focuses on core policing technology systems that were identified as the Integrated Policing Operating System (IPOS) ecosystem in the strategic business case prepared by the NSW Police Force in 2018:

- Computerised Operational Policing System (COPS)
- computer aided dispatch (CAD)
- forensics and exhibits (EFIMS)
- custody management
- major investigations and intelligence gathering (E@gle-i).

The strategic business case also identified that the NSW Police Force needed to improve system and data integration and take advantage of changes in technology such as cloud-based systems. The 2020 final business case addendum provided a schedule for critical infrastructure upgrades to support core policing systems.

During the audit period, the NSW Police Force also delivered projects under the Integrated Connected Officer (ICO) program. The ICO initiative aims to equip frontline police with real-time information and digital tools to boost efficiency, support better decision making and enhance officer safety in the field. Projects included improvements to data collection and storage from body-worn video, in-car video and automated number plate recognition. However, ICO projects fall outside the scope of this audit, as they are not considered 'core policing technologies' and were not funded through the IPOS program.

History of COPS upgrade attempts from 2007 to 2017

While this audit considers activities from 2018 to 2025, the NSW Police Force had previously attempted to upgrade core policing technology systems.

The NSW Police Force first attempted to replace COPS in 2006. Then, the NSW Police Force deemed commercially available systems too expensive, so focused on modernising the existing COPS. The operational policing program (OPP) began in 2007. It was divided into 4 phases but was only partially delivered.

OPP phases delivered between 2011 and 2014:

- 2011 – improved user interface known as WebCOPS, developed by an external provider
- 2013 – enhanced reports and search functionality in COPS, plus data security framework, also developed by an external provider
- 2014 – updated COPS custody management system, developed in-house.

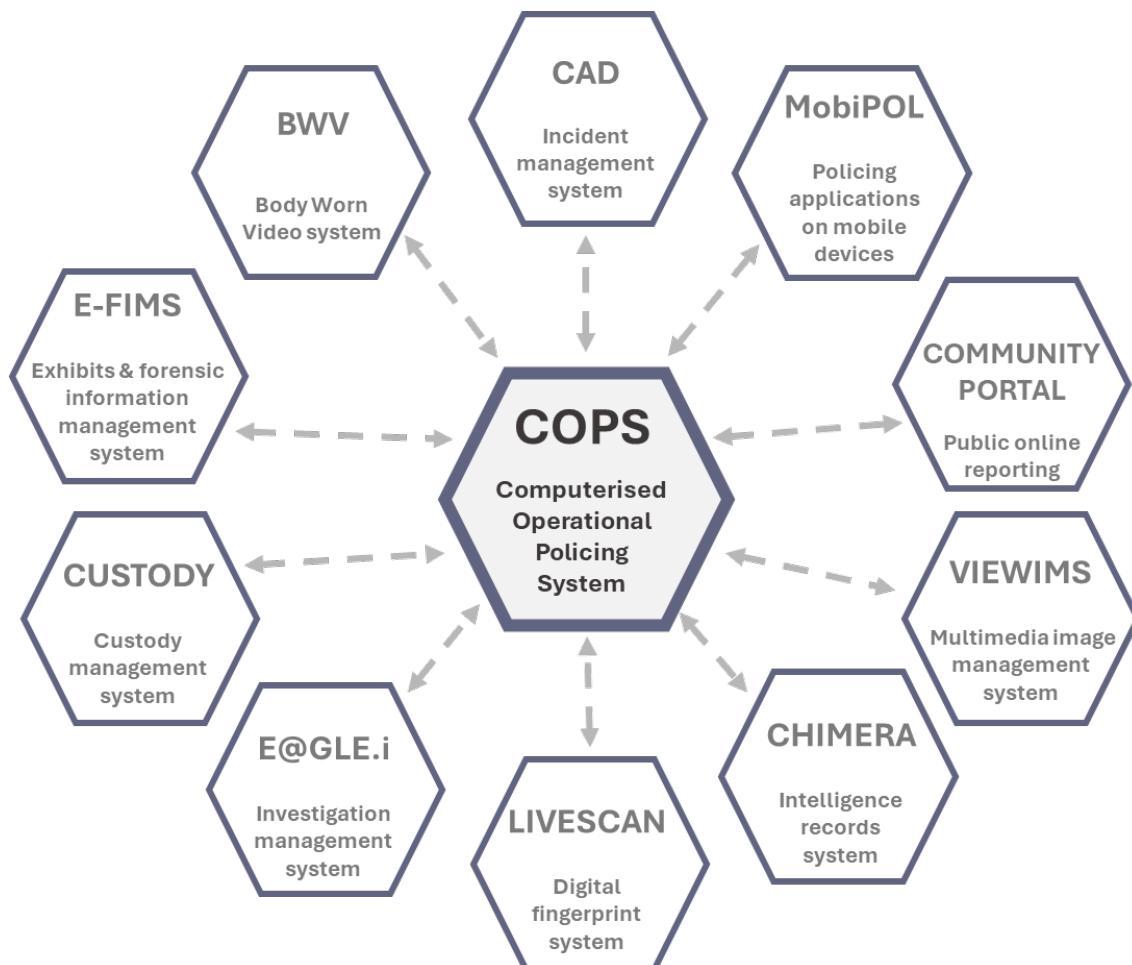
The next phase of OPP included COPS event, intelligence and case management modules, as well as a community portal. The NSW Police Force engaged external providers to design and build the system, with design work beginning in 2013 and building activities starting in 2016. The community portal went live in 2016, and a proof of concept for the COPS modules was completed in 2017.

The NSW Police Force was allocated \$45 million capital funding in 2013 to update COPS (later increased to \$49 million). The NSW Police Force prepared a revised business case in 2017 after the proof of concept for COPS modules was delivered. The business case requested \$187 million over 7 years to 2020–21 for a new COPS mainframe system, an increase of \$138 million (280%) over previous funding. The funding was not approved, so this attempt to replace COPS was abandoned in 2018, after \$36 million had been spent on the custody management system, community portal and COPS proof of concept.

Core policing systems in use in 2018

The NSW Police Force prepared a strategic business case in October 2018 that set out the need for investment in improved technology systems. It noted that there were over 300 systems and sub-systems supporting operational policing activities and 207 interfaces between COPS and internal or external systems. Figure 1 shows key policing systems in use in 2018.

Figure 1: Core policing systems in use at the time of the 2018 business case



Source: Adapted by the Audit Office of New South Wales from the NSW Police Force's 2018 strategic business case.

IPOS and Police Technology Program time periods

This audit covers a 7-year period from late 2018 to December 2025 in 3 phases:

- Initial business case and procurement – IPOS program, from October 2018 up to the termination of the primary supplier contract in June 2022 (Chapter 4)
- Transitional delivery – IPOS program, following the termination of the primary supplier contract, up to the review of program management and governance in May 2024 (Chapter 5)
- Program reset – IPOS program following program management and governance review, then re-branding as the Police Technology Program; this chapter also considers future risks to program delivery (Chapter 6).

Appendix 2 provides a summary diagram of key activities through the program phases.

4. Initial business case and procurement

In 2017, the NSW Police Force established the Integrated Police Operating System (IPOS) program to replace the Computerised Operational Policing System (COPS) and the computer aided dispatch (CAD) system, as well as forensics, investigations and custody management systems. The NSW Police Force estimated the cost to replace the COPS mainframe hardware and systems would be at least \$400 million, so instead decided to procure a 'software-as-a-service' solution by choosing the most suitable commercial off-the-shelf product.

This chapter considers the period from 2018 to June 2022, which spans procurement activities until the NSW Police Force terminated the primary supplier contract. Subsequent chapters in this report consider the later time periods.

The NSW Police Force identified the risk of maintaining legacy systems and the need for investment in core policing systems

The NSW Police Force prepared a strategic business case in October 2018 that identified the risk of maintaining legacy systems and the need for investment in core policing systems. The business case noted that the software and hardware costs were high and increasing, that the skilled programmers who maintained the existing systems were approaching retirement and that recruiting new programmers was difficult. Core policing systems were assessed as having a medium to high risk of system failure, which would have a serious impact on operational policing activities.

The strategic business case presented 3 options:

1. do the minimum – maintain existing platforms
2. IPOS – a commercial modular system provided as a suite of packages
3. hybrid – a bespoke rebuild of COPS and key satellite systems plus purchase of a commercial system for CAD.

The NSW Police Force identified option 2 as the preferred option. It assessed the technology and police operational risks as low risk, and the implementation risk as medium. The gateway review of the strategic business case concluded that IPOS was a large-scale transformation program and that the NSW Police Force needed to undertake further work to identify, assess and mitigate major risks.

The NSW Police Force conducted a thorough assessment to identify a suitable replacement for its core systems

The NSW Police Force went to market for a commercial modular system in late 2018. Between October and December 2018, the NSW Police Force narrowed down 23 proposals to 3 possible vendors through short-listing, detailed assessments and requests for additional information. The IPOS procurement documents stated that proposals should be submitted by a prime contractor and consortium partners (if required).









At the beginning of the procurement process, the NSW Police Force developed a detailed evaluation framework and a Core Tender Evaluation Committee (CTEC), comprising 10 assistant commissioners responsible for front line policing and the chief information technology officer. Functional tender evaluation teams (FTET), involving around 100 operational police staff, ICT experts, and representatives from finance, procurement and legal teams, supported the CTEC.

The NSW Police Force received 23 submissions from individual vendors and consortia, 13 organisations received full Request for Proposal (RFP) materials, and 6 complying tenders were submitted in November 2018. Following scenario demonstrations and value-for-money assessments, the NSW Police Force selected 3 vendors to progress to the next stage. In March 2019, the NSW Police Force conducted 'deep dive' sessions with the 3 vendors, which involved scenario-based demonstrations and hands-on testing.

All 3 vendors demonstrated potential efficiency savings for the NSW Police Force. One consortium was ranked first on most of the assessable factors, scoring much higher than the other 2 vendors on operational factors. The NSW Police Force decided to continue assessing all 3 vendors, because the deep dive demonstrations only accounted for 35% of the overall evaluation weighting. The remaining 65% of the weighting applied to commercial, financial and technology criteria, which were assessed through a refined RFP evaluation stage.

Table 1 summarises the NSW Police Force’s compliance with NSW Government and internal procurement policies and guidelines.

Table 1: NSW Police Force’s compliance with relevant agency and government policies and guidelines

	IPOS procurement 2019–2020
Evaluation plans were consistent with NSW Government requirements and good practice guidance	
Evaluation processes were consistent with requirements and good practice	
Evaluation plans set out clear and specific evaluation criteria	
Evaluation methodologies were consistent with NSW Police Force guidance	
Multi-level governance structures consistent with good practice were established	
Expressions of interest evaluation plan and tender evaluation plan were followed	
Independent assurance reviews consistent with the NSW ICT Digital Assurance Framework occurred at key stages	
Due diligence checks were completed on the preferred proponent	

Note:  indicates compliance with policies, procedures and guidelines  indicates partial compliance with policies, procedures and guidelines.

Source: Audit Office of New South Wales analysis of IPOS procurement documents and NSW Government procurement policies, procedures and guidelines.

In May 2019, the NSW Police Force released its refined RFP and assessed vendors through site visits and reference checks, looking at products in use in other policing agencies. Following the site visits, the consortium that scored highest during deep-dive sessions was ranked first. The evaluation also included an independent financial assessment, which rated this consortium as third. All 3 proposals were non-complying with some of the NSW Police Force’s commercial requirements, for example by not agreeing to all the responsibilities of the prime contractor. However, following independent probity advice, the NSW Police Force decided to proceed with procurement.

The NSW Police Force engaged external reviewers to support decision making and identify key risks

During the IPOS procurement process, the NSW Police Force engaged external probity advisers who reviewed documents and attended vendor demonstrations. External reviewers and evaluators identified risks in contracting with an overseas start-up firm with current and forecast losses, and no experience of contracts as large as the NSW Police Force. While the firm had delivered records management and computer aided dispatch systems to police services in the US, these were for much smaller police services with fewer functions compared with the NSW Police Force. In addition, the product did not include an existing forensics and exhibits system, which would require development of a new module rather than adapting existing software.

In September 2019, the NSW Police Force conducted a whole-of-government review focused on vendor engagement risk and invited representatives from the NSW Department of Customer Service (DCS), the NSW Department of Finance, Services and Innovation (DFSI), and the NSW Chief Procurement Officer to participate. The reviewers considered the procurement risks and how to reduce the likelihood of the risks occurring, and recommended further negotiation with the prime contractor and consortium partner before entering into contracts.

Following this review, the core tender evaluation committee concluded that the proposal from supplier A as prime contractor and supplier B as a consortium partner was the best option, scoring much higher than the other 2 viable solutions on operational criteria. The NSW Police Force considered options for contracting and sought additional legal advice. In November 2019, the NSW Police Force considered going back out to market to find a complying solution but the program steering committee decided that this would create an unacceptable delay for the project.

The NSW Police Force extended the due diligence period after risks were identified in the choice of suppliers, while changing the technical requirements caused further delays

In March 2020, the NSW Police Force selected supplier A as the prime contractor and systems integrator, with responsibility to manage end-to-end delivery of the program, including coordinating program streams, testing the product developed by supplier B and providing system security. As the prime contractor, supplier A was responsible for supplier B's performance and took on the commercial risk for the contract. The NSW Police Force entered into short-term phase 0 contracts with both suppliers to validate the RFP response, confirm scope, provide updated pricing and negotiate the final contract schedules. Before beginning phase 0 the NSW Police Force negotiated 'term sheets' with the suppliers, which set out the key commercial terms to be agreed before the contracts were signed.

The NSW Police Force extended the duration of phase 0 in the procurement process to allow for extensive due diligence. Phase 0 was originally planned to finish in September 2020, but it ran until February 2021.

During phase 0, the NSW Police Force revised the technical requirements for IPOS to increase its level of control over information and technology security. These changes included reconsideration of the original data storage and hosting location, clarification of security and sovereign ownership and responsibilities, and stronger alignment with government security requirements, including the Protective Security Policy Framework (PSPF). These changes had implications for system architecture and contractual arrangements. As a result, the NSW Police Force undertook extensive negotiations with supplier B to reassess security controls, hosting arrangements and delivery responsibilities.

Exhibit 1: Variations to supplier B's standard operations

The NSW Police Force required Supplier B to vary its standard approach.

- System and data location – supplier B's standard approach was to host the system and store data on servers located in the US. While this was suitable for its existing US-based clients, it did not meet the PSPF's security requirements. The vendor agreed to develop a NSW Police Force specific instance of the system and store it in an Azure cloud environment located in Australia.
- Location of staff – supplier B agreed to set up a team based in Sydney to work alongside NSW Police Force staff and support delivery, rather than rely only on US-based personnel.
- System source code – under supplier B's normal commercial arrangements, customers did not control the source code. The NSW Police Force required a copy of the program code to be stored in its cloud environment as a safeguard in case there were problems with the supplier.
- Delivery approach – supplier B was required to adapt its standard agile development and delivery approach by incorporating more formal planning, approval processes and milestones, consistent with NSW Government governance and assurance requirements.

Source: Audit Office of New South Wales review of NSW Police Force documents.

During the due diligence process, supplier A resigned from the prime contractor role, reducing its responsibilities and level of accountability for IPOS delivery, and proposed to continue with the systems integrator role. This increased the risk for the NSW Police Force because supplier A would no longer be responsible for supplier B's performance. The NSW Police Force accepted Supplier A's resignation from the prime contractor role but did not accept the proposal for supplier A to continue in the systems integrator role. This did not constitute a breach of contract because the program was still in the due diligence phase.

The NSW Police Force entered into a phase 1 contract for program delivery with supplier B, but not with supplier A

The NSW Police Force decided that the involvement of supplier A increased the complexity and risk of the program, especially in solution architecture. The NSW Police Force concluded that supplier A was not sufficiently familiar with supplier B's products, was not working well with supplier B, and was not providing the expected leadership in solution design and risk management. The NSW Police Force removed supplier A as systems integrator in June 2020 and took on this role itself.

The NSW Police Force implemented proactive risk management strategies in the final contract with supplier B. This included:

- a bank guarantee from supplier B
- quarterly financial health checks to provide early warning of solvency issues
- payment for actual deliverables based on milestones
- relocating staff from supplier B to Australia to deliver the program
- NSW Police Force ICT staff learning the programming code.

To limit potential financial losses, the NSW Police Force built 5 exit points into the final contract with a 'go/no-go' decision required at each stage.

The NSW Police Force prepared business cases that were informed by operational needs

The NSW Government Business Case Guidelines, administered by Treasury, assist NSW Government agencies to seek approval for capital and recurrent funding. The guidelines set out the criteria that agencies should consider, including the case for change, economic and financial analysis, and benefits expected from the proposal.

Following the 2018 strategic business case, the NSW Police Force prepared a final business case in November 2019. This identified that critical information was not available to police and partner agencies in real time and noted that ICT systems were slow and limited collaboration. The final business case concluded that legacy systems were unnecessarily complex and inhibited operational policing.

In November 2020, the NSW Police Force prepared an addendum to the final business case (FBCA). This set out the expected costs and benefits of contracting with supplier B and presented a schedule for implementing core system upgrades. The FBCA estimated that IPOS would allow operational staff to create incident records more quickly, reduce data entry into different systems and provide reliable information on mobile devices. The NSW Police Force had selected supplier B based partly on the deep-dive assessments, where supplier B scored much higher than the other 2 vendors on operational factors.

Gateway reviews had identified the risks of remaining with existing ICT systems and the risks of contracting with an overseas start-up technology firm

The NSW ICT Digital Assurance Framework, administered by the DCS, applies to major ICT projects in NSW Government agencies. Gateway reviews occur at different points through the planning and procurement of major ICT projects and provide an independent assessment of activities. Appendix 3 provides more information on reviews and health checks throughout the audit period.

The Department of Finance, Services and Innovation (DFSI) conducted 2 gateway reviews in mid-2019. The Gate 1 review, which considered strategic alignment, assessed the 3 options for replacing core systems and found that the strategic business case understated the risk of maintaining the existing platforms. The review concluded that IPOS was the only viable option. The DFSI rated delivery confidence as medium.

The DFSI conducted the next gate review (Gate 3A and Gate 4A) in July 2019. This review, which was focused on procurement, tendering approach and evaluation, assessed delivery confidence as low. It noted that the program plan was inadequately resourced and based on overly optimistic timeframes. The DFSI raised concerns that the NSW Police Force planned to select the preferred provider before finalising key commercial terms.

The DCS conducted a Gate 2 review of the IPOS final business case and addendum in December 2020, once the costs and benefits of contracting with the selected suppliers were clear. The review assessed delivery confidence as medium, which was:

driven primarily by the risks around the “new” hybrid agile/waterfall delivery approach with the NSW Police Force as the systems integrator (SI), the travel challenges imposed on the US-based supplier by the COVID-19 pandemic and the challenges of complying with [the] Protective Security Policy Framework (PSPF) when engaging a foreign vendor.

The DCS Gate 2 review of the IPOS business case raised concerns about the contract with supplier B, including a concern about fixed pricing throughout the contract duration. The review noted that ‘the IPOS Program Team needs to be vigilant to ensure that the contractual framework does not negatively impact [the supplier’s] preferred behaviours as an innovative supplier of contemporary software’. The review recommended that the NSW Police Force consider reward-sharing in future contracts.

Weaknesses in early governance and program management arrangements increased risks and hindered early program momentum

The NSW Police Force set up regular meetings from the start of the program in January 2019 for both the IPOS Program Control Group and the IPOS Steering Committee. However the gateway review during procurement in July 2019 found that the organisation did not operate effective decision making or program governance across much of the program. The review identified weaknesses in resourcing, risk and issue reporting, and overall program oversight. In response to these weaknesses, the NSW Police Force finalised a IPOS governance plan in November 2020.

The NSW Police Force also finalised a program management plan in November 2020 but did not establish a program management office until late 2021. The NSW Police Force engaged consultants to set up the program management office and to provide program management services at a cost of \$3 million from July 2021 to June 2022. The delays contributed to poor program management in the early stages of the program. The NSW Police Force advised that it had not established a program management office earlier because it was focused on procurement activities in 2019 and 2020, before funding was approved in February 2021.

In December 2021, an internal audit health check found that leadership of the IPOS program was driven by the Technology Command and not led by the business. This had reduced the delivery focus on systems that directly supported operational policing. At that time, the program steering committee included 2 deputy commissioners, one acting as the program sponsor and the other as the business owner.

The NSW Police Force did not introduce a reliable process to prioritise changes to legacy systems until 2023. During 2021 and 2022, COPS enhancements were not logged and tracked in a single system. In 2023, the NSW Police Force introduced a prioritisation board and required issues papers to accompany each request.

The NSW Police Force's inflexible recruitment processes and challenges in recruiting and retaining skilled staff affected program delivery

The IPOS risk register created in July 2019 noted that ‘an inflexible and cumbersome internal bureaucracy (i.e. HR approvals) is prohibitive to timely recruiting’; it assessed this risk as almost certain to occur. The risk register also noted that the NSW Police Force was undertaking 2 large technology projects at the same time, with higher remuneration packages for staff working on the human resource management upgrade than on IPOS.

In July 2021, the program identified challenges in recruiting business and change analysts, project managers and testing staff. In December 2021, both the chief information and technology officer and the IPOS program director resigned. By June 2022, the program risk register had recorded that ‘Multiple project resources have left the NSW Police Force, and this has caused a gap in the project resourcing and has impacted project timelines’.

The NSW Police Force received capital funding for IPOS, but this was offset by reductions in its future recurrent budget

The final business case completed in November 2019 adopted a self-funding approach, described in the DCS Gate 2 review as a ‘unique cost-neutral financing model’ drawing on existing forward allocations over 17 years.

In May 2020, the final business case was approved and in February 2021, NSW Treasury approved the release of funds. Under this model, the NSW Police Force received \$328 million in capital funding on the condition that its recurrent budget would be reduced for 11 years from 2027–28 to 2038–39.

As a result, the NSW Police Force faces a reduced recurrent expenditure budget of \$25 million in 2027–28 and \$26 million for each of the next 4 years, with these reductions already reflected in forward operating budgets. Unless the NSW Police Force receives additional funding, it will need to find savings from other operational areas to meet both these ongoing reductions and the program’s funding needs.

The NSW Police Force attempted to limit losses by terminating the contract when it was clear that supplier B could not deliver the systems

In June 2022, supplier B advised that it could not deliver a forensics and exhibits system, and that it could not deliver the minimum viable product for CAD until 2029, 6 years later than the original date in the signed contract. The NSW Police Force terminated the contract, relying on early termination clauses. This limited the contract duration and payments to the supplier, which had reached \$15 million before the contract was terminated.

In addition to payments to supplier B, the NSW Police Force had spent \$5 million on project management that provided no ongoing benefit. The total lost investment from the contract was almost \$20 million.

After the contract was terminated, supplier B began legal action against the NSW Police Force. In August 2023, the NSW Police Force and supplier B reached a legal settlement that is subject to a non-disclosure clause.

5. Transitional delivery

This chapter considers the Integrated Policing Operations System (IPOS) program after the NSW Police Force terminated its contract with supplier B in June 2022. The chapter concludes in April 2024 when the NSW Police Force reviewed the program.

After the termination of supplier B's contract, the program lacked direction and momentum

From 2022 to 2024, the IPOS steering committee met regularly, but the program lacked direction and coordination. Project teams worked largely in silos and the steering committee did not maintain sufficient oversight of timelines or budgets. During this period the NSW Police Force continued to upgrade its computer aided dispatch (CAD) system and found a suitable forensics and exhibits system but did not look for a replacement for the Computerised Operational Policing System (COPS).

Internal and external reviews also concluded that the IPOS program was unlikely to succeed. In September 2023, the Department of Customer Service (DCS) health check review rated delivery confidence as low and noted the absence of a clear delivery plan, an overarching digital policing strategy and a current business case. The review recommended that the NSW Police Force appoint a single sponsor for the program, develop a delivery plan, and update the business case and future funding model.

In September 2024, an internal audit into budget control found weaknesses in change management, budget control and executive reporting. The NSW Police Force also conducted a detailed financial reconciliation process to identify the actual capital and recurrent spending for each IPOS project, as this information had not been reported clearly to the steering committee.

The NSW Police Force hired consultants to improve program governance and project management

Following the DCS health check review, the NSW Police Force hired a member of the review team to help implement the review recommendations. This assurance and strategic adviser identified challenges with program governance and the operating model for the Technology Command, and worked with the program to clarify roles and responsibilities. The adviser worked with the program until December 2025.

In early 2024, the NSW Police Force hired consultants to review project planning and reporting. The review found that most managers for individual projects did not know or understand their budgets and were not managing them effectively. Project managers worked in silos and project plans presented different information in varied formats, which made comparison of projects difficult. The report identified that the steering committee was not maintaining effective oversight of the program budget and timelines. Exhibit 2 summarises the recommendations from the project management review.

Exhibit 2: Recommendations from the consultants' project management review

The review interviewed project managers, sponsors and key stakeholders, and assessed program documents. The report assessed the health of each IPOS project on various measures such as milestones, deliverables, resourcing, risks and governance. The review's high-level findings included:

- projects are IT focused with a disconnect between business and technology drivers
- there is a lack of consensus on program vision, success measures and benefits realisation for each project
- projects are being managed in silos rather than through an interconnected portfolio
- the command and control structure makes decision making tedious and time consuming
- there are poor project/program financial controls and inconsistency in financial management
- there is low maturity and inconsistency of quality management across projects
- there is no evidence of sourcing or ongoing assessment of project resource capability and engagement.

Source: Audit Office of New South Wales review of NSW Police Force documents.

The review recommended improving program governance so that project and program managers could make the required decisions in real time. The review team introduced consistent project management templates and provided guidance and coaching to improve the capability of project management staff.

Since 2022, the NSW Police Force has introduced only one upgraded core policing system and completed procurement for a second system upgrade

The strategic business case in 2018 identified 5 core systems to be replaced by IPOS:

- COPS
- CAD
- forensics and exhibits (EFIMS)
- custody management
- major investigations and intelligence gathering (E@gle-i).

The final business case addendum in 2020 included a schedule for decommissioning these 5 legacy systems between 2023 and 2028.

After the IPOS contract was cancelled, the NSW Police Force needed to replace EFIMS and CAD urgently because the systems were no longer fit for purpose and existing contracts were ending. In February 2025, the NSW Police Force delivered an upgraded forensics and exhibits system (NEXUS, replacing EFIMS). By December 2025, only 1 of the 5 core policing systems had been replaced. Procurement for a new CAD system was well underway, with 'go live' planned for November 2027.

In 2022, the NSW Police Force used a closed procurement approach for forensics, awarding the contract to the supplier used by all other Australian jurisdictions. The NSW Police Force then went to market in late 2022 to procure a replacement exhibits system and awarded that contract to the same supplier. The combined forensics and exhibits system, NEXUS, went live in February 2025.

After determining that upgrading the existing CAD was not cost-effective, the NSW Police Force returned to market and selected a new supplier in early 2025. In June 2025, the NSW Police Force identified potential suppliers for a replacement for COPS and included a replacement for E@gle-i as a component of this procurement.

The NSW Police Force has delivered improvements to information and communications technology infrastructure that support core policing systems

In 2018, the IPOS strategic business case identified that the NSW Police Force needed to improve its system and data integration and take advantage of changes in technology such as cloud-based systems. The 2020 final business case addendum provided a schedule for critical infrastructure upgrades to support core policing systems.

During 2020 and 2021, the NSW Police Force initiated workstreams to upgrade its information and communications technology (ICT) infrastructure, including:

- platform and security enablement (P&SE) – cloud and network services, including support for mobile devices, encryption and monitoring system usage
- integration platform and processes – enhanced exchange of information between IPOS systems and other NSW Police Force systems such as staffing, rostering and finance, and equipment used by frontline staff, for example, body-worn video, as well as integration with other agencies, including NSW courts, Transport for NSW and the Australian Federal Police
- IT service management – tools and processes to support the delivery of IPOS systems
- data management capabilities – improved data integration to provide a unified single view of policing data, plus data analytics capabilities
- testing – to ensure new and upgraded systems perform as expected.

By December 2025, the NSW Police Force had spent \$49.8 million on these ‘enabling streams’ to support core policing systems. P&SE accounted for almost two-thirds of the spending (\$32.1 million) and has delivered cloud data centres, secure data transfer between mobile devices and cloud data centres, and stronger identity management.

The NSW Police Force has also introduced several smaller system enhancements, which are likely to have improved the efficiency of operational policing

In 2023, the NSW Police Force initiated a number of smaller projects identified by operational and technical staff. The NSW Police Force advised that these projects were initially considered impractical to deliver until COPS was replaced, but ICT infrastructure improvements enabled their earlier development. The NSW Police Force revised the IPOS scope and budget to include these smaller projects. The systems were developed through a mixture of contracts and in-house development, and the NSW Police Force plans to retain them as part of the COPS replacement system.

Projects delivered included mCOPS, a mobile application that simplifies the recording of high-volume incidents such as inspections, traffic infringements and domestic violence incidents. The NSW Police Force estimates that the inspections functionality reduced average time on scene from 24 minutes to 12 minutes, and reduced COPS event creation to 2 minutes, saving the equivalent of 610 12-hour shifts in the first 18 months.

The NSW Police Force also adapted the GoodSam health responder app (renamed BluLink) to enable police to interact directly with the public through location sharing and live video. The NSW Police Force rolled out BluLink in 2024, estimating that it saved at least \$6 million in search and rescue costs in the first year.

The level of vacancies in the program and increasing contingent labour costs contributed to poor control of budgets and delays in delivering system upgrades

During 2023 and 2024, the NSW Police Force had difficulty recruiting the technical, project management and integration specialists needed to re-establish program direction. Inflexible recruitment processes and uncompetitive salary bands limited its ability to attract scarce ICT skills in a competitive labour market. In January 2023, the IPOS program had 191 approved positions, but 82 (43%) were vacant.

Throughout the program the NSW Police Force found it difficult to recruit programmers skilled in legacy technology. Specialist developers maintained the legacy systems and were integral to the IPOS data management capability workstream. The cost of temporary developers rose from \$1,000 per day in December 2021 to \$1,500 per day in December 2024, equivalent to \$345,000 per year. In May 2024, the project management report found that prolonged vacancies in key technical roles had impacted the design and delivery of IPOS. Steering committee papers frequently reported that program vacancies contributed to poor control of budgets and delays in delivering system upgrades.

6. Program reset

This chapter covers the time period after the Integrated Policing Operations System (IPOS) program was reviewed in mid-2024, and then rebranded as the Police Technology Program (PTP) in late 2024. The chapter also considers the state of the program in December 2025 and the risks the NSW Police Force must address as procurement progresses and systems are implemented.

In 2024, the NSW Police Force merged 2 commands and made changes to IPOS governance arrangements to improve project planning, budget control and decision-making processes

In May 2024, the NSW Police Force merged the Technology Command and the Communication Services Command. This resulted in a change of leadership for technology programs and provided an opportunity to reset the IPOS program. From July 2024, the NSW Police Force began implementing recommendations from the gateway review and project management report, including moving to a single sponsor for IPOS and making changes to governance arrangements.

Following the project management review, internal audit report and financial reconciliation exercise in mid-2024, the NSW Police Force developed consistent project plans and tracking for each IPOS project. During 2024, it also strengthened the governance of the Computerised Operational Policing System (COPS) replacement workstream and aligned it with the mainframe and application data decommissioning (MADD) project.

In September 2024, the DCS conducted a second health check review, which rated delivery confidence as medium, and noted improvements in leadership, governance structures and early delivery outcomes.

The NSW Police Force has significantly improved the governance of the program and the quality of project management

Following the merger of the Technology Command and the Communication Services Command in May 2024, the NSW Police Force improved its information and communications technology (ICT) maturity and developed a digital strategy. It strengthened governance through the PTP steering committee, which included representatives from several operational commands and the new Technology and Communication Services Command (TCSC). The committee was chaired by the PTP program sponsor, the Deputy Commissioner, Corporate Services, and had clear terms of reference.

Since April 2025, the steering committee has received more consistent and structured reporting for each PTP project, covering delivery status, financials, risks/issues/dependencies, benefits realisation and change management. The steering committee papers also detail the actions needed to move a project's status from amber or red to green. This has improved transparency and supported better oversight of projects and decision making.

In November 2025, the NSW Department of Customer Service (DCS) conducted a health check review, which identified improvements in the program and rated overall delivery confidence as medium. The review assessed key scope areas, rating both the current phase and readiness for the next phase as high, and the delivery approach and risk management as medium.

The NSW Police Force does not expect to deliver the full suite of upgraded systems until 2031, 4 years after the program's original end date

Although the NSW Police Force identified the COPS replacement as its highest priority for the rebranded PTP, the delivery timeline for phase 1 of the core policing solution is now June 2029. The timeline for delivering future modules, including intelligence management and custody management, is June 2031, 4 years after the original IPOS end date.

When the NSW Police Force prepared the full business case for IPOS in 2020, it expected to implement 2 core policing systems: computer aided dispatch (CAD) and forensics by June 2023; and replacement COPS modules covering report writing, investigations and inspections by June 2025. The final core policing systems, including custody management, major investigations and legal process, were due by June 2027. In November 2024, the NSW Police Force determined that the program could not be delivered by June 2027 and the end date was extended to June 2029.

In June 2025, the IPOS steering committee was advised that \$24.3 million had been transferred from the IPOS capital budget in 2025–26 to Infrastructure and Assets Command for the purchase of Mascot police station, with funds to be repaid in 2027–28 and 2028–29. The transfer of funds was approved by the Commissioner’s Executive Team and NSW Treasury, and extended the timeline for IPOS delivery by 2 years from June 2027 to June 2029, which better aligned with the NSW Police Force’s capacity to deliver the program.

In October 2025, the NSW Police Force prepared a revised business case for the PTP. This shows that phase 1 of the PTP, due by June 2029, includes several core policing systems, notably forensics and exhibits, CAD and 2 modules of the core policing solution (crime recording and investigation management). PTP phase 1 combines systems already delivered with systems where procurement was still underway.

Phase 2 of the PTP, due by June 2031, includes the remaining modules from the COPS replacement system, namely information and intelligence management, procedural justice, regulatory services, crime prevention and public safety. Phase 2 also includes modernisation of the firearms licensing system. Appendix 3 provides more information on the status of PTP projects at December 2025.

The NSW Police Force had spent over \$155 million on core system projects and supporting ICT infrastructure, but major components are outstanding

By December 2025, the NSW Police Force had spent over \$155 million of the \$328 million capital budget, including: \$36 million for forensics and exhibits; \$32 million for cloud hosting and security; \$18 million on other ICT infrastructure projects; \$16 million on upgrading legacy systems; \$19 million on ancillary systems, such as mCOPS; and \$9 million on CAD.

The \$50 million spent on cloud hosting, security and other ICT infrastructure projects was critical capital expenditure to support current delivery and future capabilities, such as CAD and the core policing solution project. While the NSW Police Force expects to deliver an upgraded CAD system in 2027, the timeline for core policing system modules cannot be determined until procurement is completed.

By December 2025, the NSW Police Force had spent \$11 million on project and program management services and \$9 million on system architecture services. The NSW Police Force had spent almost \$18 million on consultants and contractors to support the IPOS program. The largest payments were \$4.85 million to supplier A for phase 0 due diligence in 2020 and \$3.6 million to consultants for program management services in 2021 and 2022.

The NSW Police Force estimates that delivering the PTP will cost an additional \$78 million in capital funding by 2031

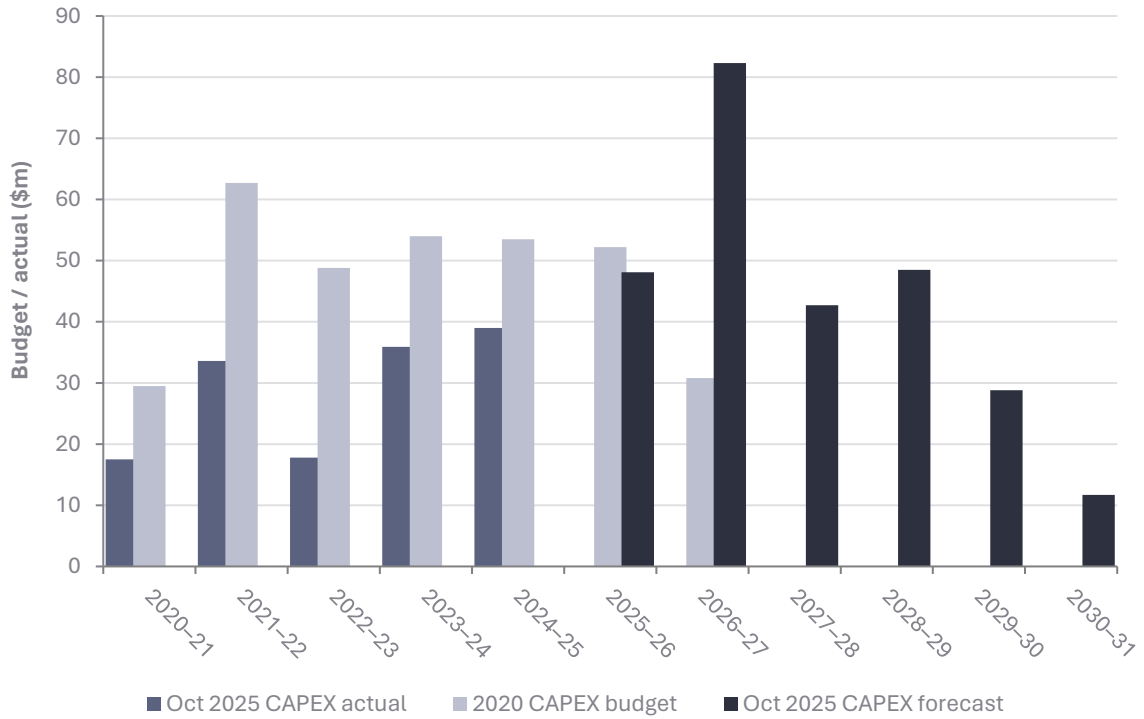
The revised PTP business case indicated that \$184 million of the original \$328 million capital allocation remained available for system development at 30 June 2025, but this was insufficient to fund the full program.

The DCS reviewed the business case in October 2025, and it was subsequently endorsed by the Commissioner’s executive team (CET). The NSW Police Force planned to submit it to Treasury in early 2026. At February 2026, the NSW Police Force had not presented a final business case to inform government that additional funding would be needed and that the delivery timeline is now 2031.

The NSW Police Force estimates that PTP phase 1 will cost a further \$150 million to complete CAD, forensics, mobile systems and the modernisation of COPS investigation management modules. While phase 1 can be funded from within the approved capital allocation, phase 2 requires additional capital investment totalling \$78 million. PTP phase 2 aims to deliver the remaining modules of the core policing solution and the firearms licensing modernisation project.

Exhibit 3 shows the capital budget presented in the 2020 business case, the actual capital expenditure incurred by the NSW Police Force from 2019–20 to 2024–25, and the revised capital expenditure forecast reported in the 2025 business case.

Exhibit 3: IPOS capital expenditure – Budget in 2020 compared with IPOS/PTP actuals to 2024–25 and revised budget to 2030–31



Source: Audit Office of New South Wales review of NSW Police Force documents.

Forecast recurrent expenditure costs have increased markedly since 2020 and the NSW Police Force will need at least \$380 million in recurrent spending on core ICT solutions by June 2031

The revised business case identified high ongoing recurrent funding requirements due to software licences and data storage and access costs. It noted that as more systems move to cloud-based and subscription-based services, expected costs shift from one-off capital spending to recurrent funding models. While these subscription services improve flexibility, agencies need reliable ongoing funding to maintain service levels and avoid service gaps.

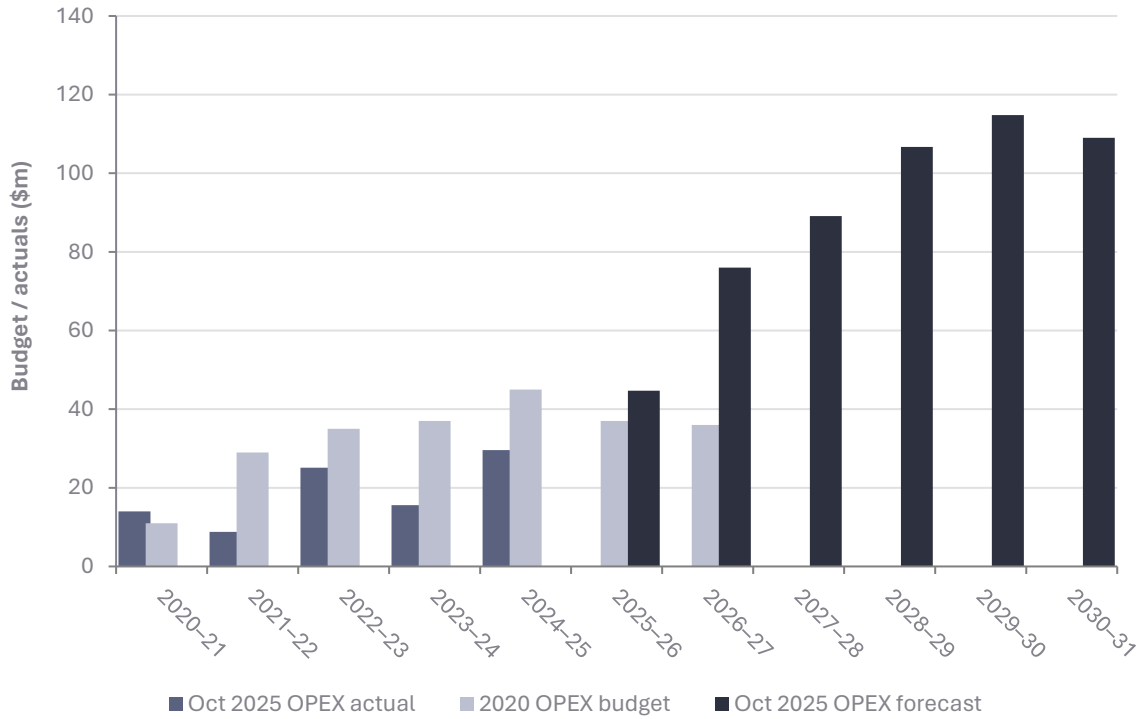
In the business case prepared in 2020, the NSW Police Force estimated that IPOS would require recurrent expenditure of \$35 million per annum on IPOS products delivered by supplier B. The consistent cost resulted from the contract that NSW Police Force had negotiated, which did not include any consumer price index increases through to 2038. In addition, the NSW Police Force budgeted for recurrent expenditure on supporting ICT infrastructure and maintaining legacy systems during the IPOS rollout.

The NSW Police Force prepared new estimates of recurrent expenditure in the 2025 program business case, totalling \$389.4 million from July 2026 to June 2031. In addition, it estimated recurrent costs for legacy systems of around \$25 million per year.

In 2025, the NSW Police Force estimated a recurrent funding gap of \$415 million up to June 2031. This included \$129 million in reduced future recurrent costs from July 2027 to June 2031, approved in the 2020 IPOS business case. The funding gap also included the costs of running the legacy systems for an extra 4 years, which the NSW Police Force estimated to be \$88 million more than previously budgeted. The business case restated the imperative of investing in PTP, despite the cost, and noted that doing nothing was not an option.

Exhibit 4 shows the recurrent expenditure budget presented in the 2020 business case, the actual recurrent expenditure incurred by the NSW Police Force from 2019–20 to 2024–25 and the revised recurrent expenditure forecast reported in the 2025 business case.

Exhibit 4: IPOS recurrent expenditure – Budget in 2020 compared with IPOS/PTP actuals to 2024–25 and revised budget to 2030–31



Source: Audit Office of New South Wales review of NSW Police Force documents.

The NSW Police Force plans to maintain legacy systems for at least 4 years longer than expected

The NSW Police Force originally planned to replace the mainframe system by 2027, but the system is now required until at least 2031. The mainframe costs the NSW Police Force approximately \$13 million per year for hardware and mainframe software, plus an additional \$8 million per year for software licences. This expenditure is wholly to maintain continued operation of legacy systems and is of no benefit to future operating systems.

In 2024, the NSW Police Force spent \$2.7 million replacing the mainframe hardware that supports COPS and relocating the mainframes to a new location. This was outside the scope of the original business case. The 2020 business case assumed that decommissioning the mainframe would save around \$26 million per year from July 2027 onwards. The mainframe has not yet been decommissioned, and the NSW Police Force no longer expects savings when this happens.

The NSW Police Force expects to spend \$6.8 million on staffing over 4 years to support the obsolete technology. The NSW Police Force advised that these roles are required to implement legislative changes and ensure continuity of critical services, regardless of the underlying technology. However, updating the COPS mainframe systems is more time-consuming than updating more modern technology. For example, in 2023, the NSW Police Force improved the reporting of bushfires, structural and other fires in COPS, including creating a separate incident category for bushfires. This COPS development work required 110 days of developer time due to the complexity of working in a legacy system.

Exhibit 5 summarises capital expenditure to June 2025 on ‘refresh and resilience’ (R&R) projects, which aimed to provide short-term improvements to legacy systems that were expected to be replaced by the COPS upgrade.

Exhibit 5: R&R projects

Delays in implementing IPOS resulted in additional costs for legacy systems. The final business case addendum from 2020 included \$12 million capital funding for R&R projects, described as ‘a program of work to replace, enhance or support core IT capabilities until these systems are replaced’, that is, until IPOS was implemented. There were 4 separate R&R projects:

1. a major investigations system (CRIME)
2. a homicide investigations management system (HIMS)
3. a covert operations database (COD)
4. spatial capability.

By December 2025, the NSW Police Force had spent \$13.7 million on the R&R projects and had not delivered a replacement for the major investigations system (including the HIMS). The NSW Police Force developed Power BI reports for the unsolved homicides team in early 2025 to address business needs that were unmet by the existing legacy system. COD phase 1 was delivered in January 2025 and, in August 2024, improvements in spatial capability transferred to business-as-usual.

Source: Audit Office of New South Wales review of NSW Police Force documents.

Continued reliance on legacy systems exposes the NSW Police Force to technology risk and reduces operational effectiveness

The NSW Digital Strategy identifies that government agencies must reduce legacy technology and duplication of digital solutions. Following the replacement of mainframe hardware in 2024 and relocation to a more secure location, the NSW Police Force considered that the hardware risk had been addressed in the medium term. However, the mainframe applications still in use, including COPS, result in inefficient processes for operational staff. The program business case prepared by the NSW Police Force in October 2025 identified inefficiencies including:

- legacy systems require officers to enter the same information more than once, increasing administrative workload
- older, non-mobile interfaces mean officers need to return to stations to input data, reducing the time available for work in the community
- staff often use inefficient, paper-based processes to overcome problems with COPS
- systems are not well integrated, so officers often need to switch between different systems to complete routine tasks, increasing the risk of mistakes.

The NSW Police Force concluded that continuing to rely on legacy applications increased the risks of service interruptions and cyber security incidents and could impact public safety. It also noted that because COPS underpins many policing functions, system failures could disrupt frontline policing operations.

The NSW Police Force faces continuing challenges in recruiting technical staff to support its legacy systems. In December 2024, the TCSC requested 10 temporary positions within the core policing team. These staff would learn the specialist legacy system programming language to enable them to maintain and make changes to COPS and ensure business continuity for the NSW Police Force. The total cost of these staff was \$1.723 million per year.

Exhibit 6 provides a case study from 2019 summarising the challenges for operational staff using legacy systems. While the exhibits system was upgraded in February 2025, a replacement for COPS has not yet been delivered.

Exhibit 6: Case study demonstrating operational impact of legacy systems

In July 2018, detectives from the NSW Police Force Financial Crimes Squad and Organised Crime Squad, along with the Australian Government Department of Education and Training and the Australian Criminal Intelligence Commission (ACIC), established Strike Force Mercury to investigate coordinated fraudulent activities targeting family day care operations.

In May 2019, Strike Force Mercury arrested 18 people simultaneously and executed 23 search warrants in relation to a \$4 million fraud. The outdated IT infrastructure used by the NSW Police Force significantly increased the resources required and time taken to input and process data. For example:

- one master event was created in COPS with 23 search warrant incidents; only one police officer could update the event at a time
- 18 events were created for the arrests, requiring 18 police officers to process offenders
- 700 exhibits were seized, photographed and manually entered into 4 different systems
- search warrant documents and operation orders were manually entered into 5 different systems, which had to be done retrospectively as there was no scope for entering the information in real time.

Source: Audit Office of New South Wales review of NSW Police Force documents.

The NSW Police Force has incorporated lessons from previous procurement experiences and updated its contracting approach

The NSW Police Force has moved away from a single vendor approach and expects to contract with multiple vendors for the remaining components of PTP. This approach was endorsed through an independent assessment in July 2025. The DCS health check in November 2025 rated confidence in the delivery approach as medium and noted that 'PTP has pivoted to a more flexible and scalable delivery model'.

Procurement processes conducted in 2024–25 (next gen CAD and COPS replacement) required tenderers to meet minimum staff and revenue thresholds, effectively excluding start-up firms. Proposals were only accepted from companies with experience in the Westminster system of government that also complied with the Australian Protective Security Policy Framework. The NSW Police Force determined that a commercial off-the-shelf (COTS) product would not be sufficiently adaptable for COPS, given the need to implement legislative changes quickly. Revised Treasury guidelines now advise agencies to stage the delivery of large programs and request smaller funding tranches.

In November 2024, the NSW Police Force issued a premarket notice to restart the procurement process for a replacement for COPS. It included 7 capabilities, covering operational policing processes plus ICT infrastructure and data analytics.

In July 2025, the NSW Police Force presented the PTP strategic delivery approach to the CET. This identified lessons from the IPOS program, assessed changes in technology and Treasury guidelines, then outlined a different approach for PTP. Exhibit 7 summarises the lessons learnt by the program, including lessons that may be applicable to other NSW Government agencies.

Exhibit 7: Lessons learnt

NSW government agencies should:

- adopt a multi-vendor, best-fit solution model, using the most appropriate technology for each capability rather than rely on a single vendor
- recognise that generic COTS solutions are unlikely to scale for large NSW agencies without extensive and costly customisation
- identify and actively manage risks arising from cross-program dependencies, including those within and outside program workstreams
- actively challenge optimism bias, regularly reassessing assumptions about cost, timeframes, vendor capability and internal capacity
- embed service design and user experience from the outset, with ongoing involvement of end users throughout delivery
- build and sustain internal delivery capability and culture, so agencies are equipped to lead complex, long-running programs
- ensure strategic trade-offs are clearly identified and documented, to balance urgent operational needs against long-term technology outcomes
- use commercial models with clear stage gates and exit options, to manage uncertainty and protect value in large digital programs.

The NSW Police Force should:

- select systems designed for Westminster-style policing in large, complex jurisdictions, rather than adapt products built for different policing models
- ensure it leads program design, governance and decision making, with vendors supporting delivery rather than directing it.

Source: Audit Office of New South Wales review of NSW Police Force documents.

The NSW Police Force will require strong governance, effective decision making and senior manager support to meet PTP timeframes, with key person reliance remaining a program risk

Throughout the audit period, gateway reviews, health checks and consultant reports have raised issues about poor project management, slow decision making, and challenges in recruiting and retaining skilled staff.

Since November 2024, the NSW Police Force has made progress in addressing these issues and strengthening governance arrangements. This has been supported by experienced project sponsors and staff across the organisation. However, the program remains vulnerable to setbacks if key personnel leave or change roles.

The DCS health check review in November 2025 reported that ‘securing key resources will be essential to maintaining delivery pace and achieving program objectives on schedule’. One of the 2 critical recommendations related to recruiting appropriately skilled program staff and noted that this ‘may require remuneration decisions to meet the market’. The health check review also noted the importance of ensuring continuity of key personnel with accountability for project deliverables, through program development and implementation phases.

In November 2025, the PTP steering committee monitored risks related to ‘protracted and delayed decision-making processes’ and poor-quality project documentation, which both had high residual risk ratings after mitigation.

The NSW Police Force received funding in the 2025 NSW budget for critical network upgrades. These upgrades are expected to be delivered at the same time as PTP projects and require ICT specialists and project management staff with scarce skills. Delivering major projects on time and on budget will continue to be a significant challenge for the NSW Police Force.

The NSW Police Force has identified insufficient funding as a key risk to program delivery

In July 2024, the PTP steering committee identified insufficient capital and recurrent funding as a key risk. The risk action plan included preparing the business case addendum to request additional funding from Treasury and implementing rigorous financial oversight of project activities, but the risk rating remained high after mitigating actions. The risk remained on the PTP risk register in November 2025.

The October 2025 program business case noted that changes to the technology environment, especially the move to software-as-a-service and higher licensing costs, had resulted in increased recurrent expenditure needs to June 2031. The business case noted that wage pressures and inflation had also affected delivery costs. The original IPOS business case was approved by government in May 2020; it took the NSW Police Force over 5 years to submit a revised estimate of funding needs.

The DCS health check in November 2025 rated the business case and stakeholders key scope area as low, due to uncertainty over funding to complete the program. The DCS recommended that the NSW Police Force consult with NSW Treasury about additional funding, and update cost and benefits estimates in the business case.

If additional capital funding is not approved for the PTP, the NSW Police Force advises it will not be able to deliver all the modules of the core policing solution. If additional recurrent expenditure is not approved for cloud services and software-as-a-service, the NSW Police Force will need to fund increased recurrent expenditure for PTP by identifying savings elsewhere within the organisation.

Appendix 1 – Response from entity

Response from the NSW Police Force

Official



NSW Police Force

OFFICE OF THE COMMISSIONER

24 April 2026

Mr Bola Oyetunji
Auditor-General for New South Wales

By email: mail@audit.nsw.gov.au

Dear Mr Oyetunji,

Response to Performance Audit Report on Upgrades to Core Policing Technology

I write to acknowledge receipt of the Performance Audit Report titled Upgrades to Core Policing Technology and to thank the Audit Office of NSW (Audit Office) for its examination of the NSW Police Force's planning, procurement and governance arrangements relating to the replacement of core policing technology systems.

The NSW Police Force acknowledges the report's findings regarding shortcomings in earlier phases of the program, including challenges associated with legacy systems, supplier non-performance and governance arrangements following the termination of the primary contract in 2022. We recognise the Audit Office's role in providing independent assurance to Parliament and welcome the opportunity to formally respond.

The report appropriately notes that the NSW Police Force has long recognised the operational, financial and technology risks associated with ageing core systems, particularly COPS, and that successive business cases since 2018 have documented the necessity of large-scale transformation. The NSW Police Force recognises that earlier delivery approaches did not achieve the intended outcomes within the original timeframes.

It is, however, important to emphasise that the operating model, delivery approach and governance arrangements assessed in earlier phases of the audit are fundamentally different to those currently in place. From early 2024, the NSW Police Force initiated a comprehensive reset of the program, now known as the Police Technology Program (PTP). This reset was designed to limit further exposure and preserve service continuity and included the introduction of single accountable sponsorship, a phased and capability-based delivery model, a move away from a single-vendor approach, strengthened financial oversight, and reinforced independent assurance.

The Audit Office's report reflects that these changes have materially improved governance, transparency and delivery confidence. Independent health checks conducted in 2024 and 2025 have also assessed

Locked Bag 5102 Parramatta NSW 2124 [W www.police.nsw.gov.au](http://www.police.nsw.gov.au) TTY 02 9211 3776 for the hearing and speech impaired ABN 43 408 613 180

TRIPLE ZERO (000)

Emergency only

POLICE ASSISTANCE LINE (131 444)

For non-emergencies

CRIME STOPPERS (1800 333 000)

Report crime anonymously

Official

Official

the program's current position and next-phase readiness positively. These reforms represent more than incremental improvement; they constitute a fundamental restructuring of how technology transformation is governed and delivered within the NSW Police Force.

The NSW Police Force notes the report's recognition that significant operational capability and foundational infrastructure have been delivered since funding approval in 2021, while observing that the report places greater emphasis on historical challenges than on the material improvements achieved since 2024.

Despite early delivery and governance issues, the investment to date has delivered critical platforms and enabling infrastructure to stabilise operations, strengthen cyber security, modernise hosting and integration, and reduce risk ahead of replacing mission-critical systems. These improvements have delivered tangible benefits to frontline policing, including improved system reliability, enhanced mobility and access to information, and strengthened security. These outcomes—including forensics and exhibits, mobile policing, cloud hosting, cyber security uplift and integration capability—were deliberately prioritised as essential dependencies for the safe replacement of complex systems such as CAD and the core policing solution.

Many of the challenges identified in the report arose during a period of significant and well-documented reform across government and the information and communications technology (ICT) sector. This period was marked by a whole-of-government reassessment of technology delivery models, including growing recognition that large, monolithic commercial off-the-shelf platforms were often ill-suited to the complexity and risk profile of public sector operating environments. It also coincided with sustained growth in recurrent ICT costs associated with cloud adoption, expanding data volumes, and heightened cyber security and privacy obligations, as well as changes to public sector accounting and financial management frameworks that affected the timing and visibility of operating expenditure. These sector-wide developments influenced technology programs across many agencies and drove shifts towards phased delivery, modular architectures, strengthened assurance, and clearer articulation of whole-of-life costs and funding assumptions, which are reflected in the NSW Police Force's revised delivery approach.

The report identifies that full delivery of the program is now expected by 2031 and that additional capital and recurrent funding will be required. The NSW Police Force acknowledges these findings and notes that the revised delivery timeline and funding profile are directly linked to the broader sector-wide changes outlined above. The revised delivery timeline and funding profile reflect a deliberate and strategic re-baselining undertaken following the program reset, informed by more realistic assumptions, contemporary assurance standards, inflationary impacts and a revised multi-vendor commercial approach.

These matters are addressed in detail in the revised business case and supporting financial analysis, which has been validated through engagement with the Audit Office.

The NSW Police Force remains committed to disciplined program governance, transparent financial management, and the successful delivery of secure, modern technology that supports frontline policing and public safety.

Locked Bag 5102 Parramatta NSW 2124 [W www.police.nsw.gov.au](http://www.police.nsw.gov.au) TTY 02 9211 3776 for the hearing and speech impaired ABN 43 408 613 180

TRIPLE ZERO (000)

Emergency only

POLICE ASSISTANCE LINE (131 444)

For non emergencies

CRIME STOPPERS (1800 333 000)

Report crime anonymously

Official

Official

The NSW Police Force accepts the Audit Office's recommendations and supports their intent. A detailed response to the findings and recommendations is provided below.

I would like to thank the Audit Office for its engagement with NSW Police Force staff throughout the audit process.

Yours sincerely



M A Lanyon APM
Commissioner of Police
NSW Police Force

Locked Bag 5102 Parramatta NSW 2124 [W www.police.nsw.gov.au](http://www.police.nsw.gov.au) TTY 02 9211 3776 for the hearing and speech impaired ABN 43 408 613 180

TRIPLE ZERO (000)

Emergency only

POLICE ASSISTANCE LINE (131 444)

For non emergencies

CRIME STOPPERS (1800 333 000)

Report crime anonymously

Official

Response to the Recommendations

Recommendations	Response	Commentary
<p>1. Demonstrate effective program governance arrangements that:</p> <p>a) support delivery of the police technology program in line with planned milestones</p> <p>b) maintain robust budget controls to align spending with approved funding and scope, and to ensure early identification and management of variances</p> <p>c) achieve intended outcomes by driving clear accountability, effective oversight of delivery risks and assessment of value for money</p> <p>d) ensure effective management of technology-enabled transformation and organisational change</p> <p>e) ensure the required capability is maintained</p>	Accepted	The NSW Police Force will continue to demonstrate effective governance arrangements to support the delivery of the police technology program including a maintaining budget controls, delivery risks and organisational change.
<p>2. Apply lessons learned from the early procurement and program management experience to the program, particularly in relation to procurement capability, supplier selection and early intervention where delivery risks emerge.</p>	Accepted	The NSW Police Force will continue to leverage off lessons learned through this project and other key deliverables.

Response to the Key Findings

Key Findings	NSW Police Force Response
Program delays mean that operational, financial and technology risks identified in the	The NSW Police Force acknowledges that prolonged reliance on legacy systems has continued to present operational and technology risks. However, the 2018 Strategic Business Case was intentionally high-level and

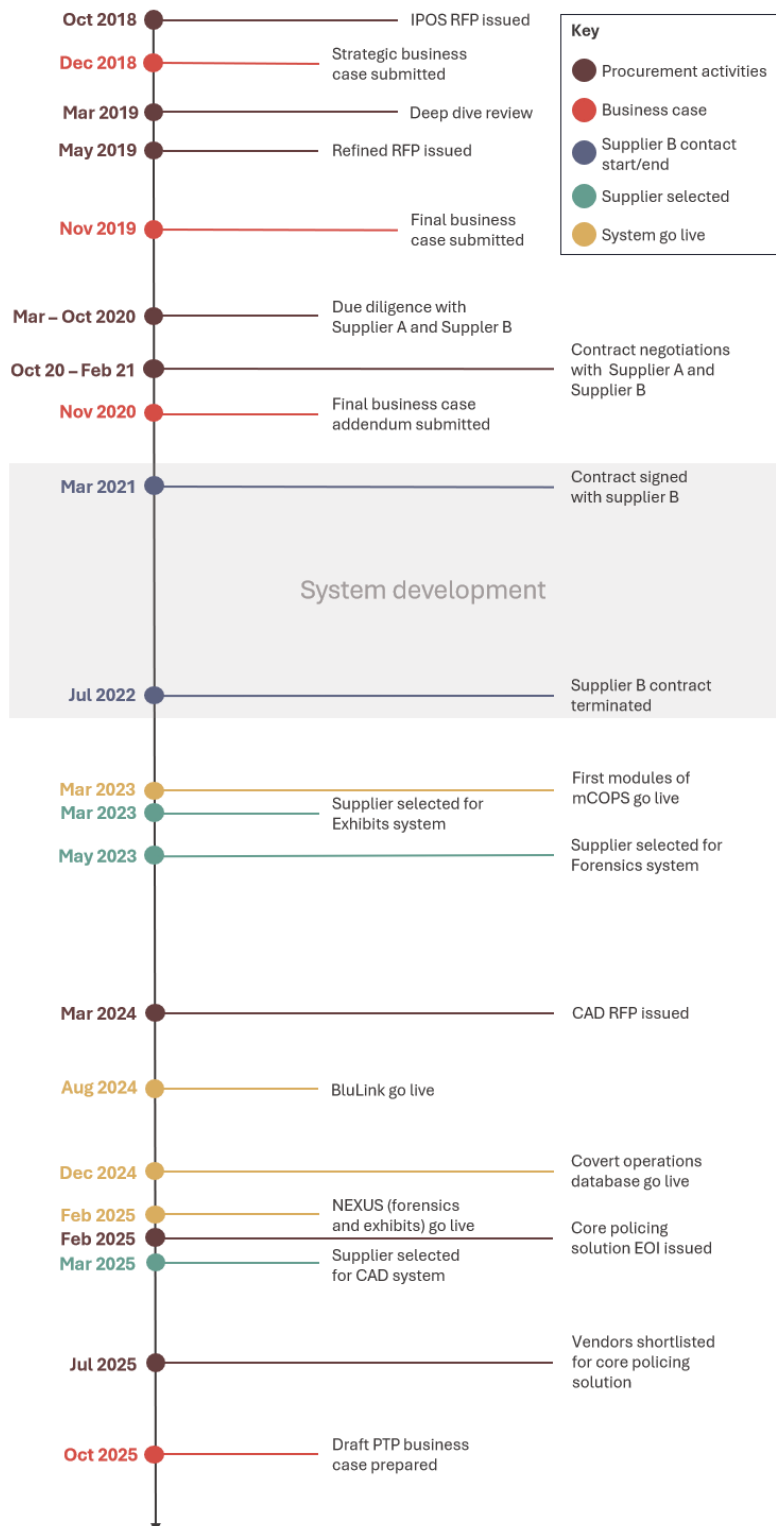
<p>2018 strategic business case remain unaddressed.</p>	<p>did not define delivery sequencing. The subsequent 2019 Full Business Case articulated a broader scope, including critical enabling capabilities.</p> <p>Since funding approval in 2021, the NSW Police Force has delivered essential infrastructure, security uplift and operational capabilities consistent with approved scope. In 2024, the program was re-baselined as the Police Technology Program (PTP) using a phased, capability-based delivery model, materially changing how risk reduction and progress are managed.</p>
<p>Despite a thorough procurement process, the NSW Police Force selected a supplier identified as high risk and developed mitigation strategies to reduce contract risk.</p>	<p>The NSW Police Force accepts that the selected supplier ultimately failed to deliver key capabilities. The procurement process itself was compliant, competitive and supported by probity advice, Gateway reviews and scenario testing. Identified delivery and capability risks were documented, accepted with executive oversight, and actively managed through contractual controls and staged exit points. Supplier non-performance triggered contract termination in 2022, consistent with prudent contract management to limit further exposure.</p> <p>The NSW Police Force has since reformed its procurement approach, moving to a multi-vendor delivery model with stricter capability and experience thresholds.</p>
<p>The NSW Police Force has delivered several systems and upgraded essential ICT infrastructure.</p>	<p>The NSW Police Force agrees with this finding. Since funding approval, the NSW Police Force has delivered or partially delivered multiple systems and foundational enabling streams, including forensics and exhibits, mobile policing solutions, cloud hosting, cyber security and system integration.</p> <p>These outcomes were deliberately prioritised to stabilise the operating environment, deliver frontline benefit and reduce delivery risk ahead of replacing mission-critical systems such as CAD and the core policing solution.</p>
<p>The NSW Police Force reset program governance and delivery arrangements in 2024, addressing weaknesses experienced earlier in the program, however key person reliance remains a risk.</p>	<p>The NSW Police Force agrees that governance and delivery arrangements were significantly strengthened through the 2024 program reset. Improvements commenced in early 2024 and included single sponsorship, standardised reporting, strengthened financial oversight, independent assurance and a revised delivery model. Independent health checks in 2024 and 2025 assessed delivery confidence for the current phase and next-phase readiness positively.</p> <p>The NSW Police Force acknowledges that key person reliance remains a risk and is actively managing this through workforce planning, capability uplift and assurance mechanisms.</p>

<p>Full delivery is not expected until 2031, 4 years after the originally identified end date.</p>	<p>The NSW Police Force acknowledges the revised delivery timeframe. The 2031 date reflects a deliberate re-baselining following the 2024 program reset, informed by lessons learned, changed delivery strategy and contemporary assurance expectations. It represents a new phased delivery baseline rather than delay against an unchanged plan.</p> <p>Continued operation of legacy systems has been a deliberate risk-management decision to ensure service continuity while replacement capabilities are progressively delivered.</p>
<p>The NSW Police Force has estimated it will require additional capital and recurrent funding to complete the program due to rising costs, a change in strategy and earlier incorrect assumptions.</p>	<p>The NSW Police Force agrees that additional capital and recurrent funding is required to complete delivery. The revised funding profile is supported by the 2025 business case addendum and reflects corrected assumptions from the 2019–20 business case, inclusion of BAU and legacy costs, inflationary impacts and higher costs associated with a multi-vendor delivery strategy.</p> <p>Financial information has been reconciled and validated through SAP, program governance reporting and engagement with the Audit Office.</p>

Appendix 2 – Timeline of key events

Figure 2 shows key events in the program from October 2018 to December 2025, categorised by type of activity, for example, procurement activities or system go-live dates.

Figure 2: Summary of key activities from 2018 to 2025



Source: Audit Office of New South Wales review of NSW Police Force documents.

Appendix 3 – Gateway reviews and health checks

Major information and communications technology (ICT) projects in NSW Government agencies are governed by the NSW ICT Digital Assurance Framework, administered by the NSW Department of Customer Service (DCS). Until 2020, gateway reviews were conducted by the NSW Department of Finance, Services and Innovation (DFSI). Gateway reviews occur at different points through the planning and procurement of major ICT projects and provide an independent assessment of activities.

Between 2019 and 2025, there were 7 independent reviews of the program plus one health check conducted by the NSW Police Force internal audit team. Table 2 summarises the reviews and shows that delivery confidence was mostly rated as medium up to early 2021, fell to low in 2022 and 2023, then returned to medium in 2024 and 2025.

Table 2: Integrated Police Operating System (IPOS) and Police Technology Program (PTP) gateway reviews and health check reviews

Date	Report	Author	Delivery confidence
May 2019	Gate 1 review: Strategic business case	DFSI	Medium
July 2019	Combined Gate 3A and Gate 4A review: Procurement, tendering approach and evaluation	DFSI	Low
December 2020	Gate 2 review: Business case	DCS	Medium
February 2021	Gate 4 review: Final tender evaluation	DCS	Medium
February 2022	Major program platform review: IPOS health check	NSW Police Force Internal Audit	Low
September 2023	IPOS health check 2 review	DCS	Low
September 2024	IPOS health check 2 review	DCS	Medium
November 2025	PTP health check review	DCS	Medium

Source: Audit Office of New South Wales review of NSW Police Force documents.

May 2019: Gate 1 review – Strategic alignment

This review assessed the 3 options for replacing core systems and considered that the strategic business case understated the risk of maintaining the existing platforms. The review highlighted that a major failure of the existing ICT systems could severely affect frontline policing operations. The review concluded that options 1 and 3 were both unpalatable and that IPOS was the only viable option. The DFSI rated delivery confidence as medium.

July 2019: Gate 3A & Gate 4A review – Procurement, tendering approach and evaluation

This review was less favourable than the Gate 1 assessment, giving a low rating for delivery confidence. It found that the program plan lacked sufficient resources and set overly ambitious timeframes. Additionally, the broader NSW Police Force had not yet committed adequate resources or shown clear prioritisation of this essential business transformation initiative.

The DFSI raised concerns that the NSW Police Force planned to select the preferred provider before gaining agreement to core commercial terms and recommended adding exit points to the contracts in case of supplier non-performance.

The review found that the program lacked effective decision making and governance. It highlighted issues such as inadequate communication regarding changes to the request for proposal timetable, delays in hiring experienced program staff, and shortcomings in reporting risks and issues to the steering committee and other key stakeholders.

December 2020: Gate 2 review – IPOS final business case and addendum

The aim of the Gate 2 review was to assess whether the full business case was robust, contained plans to realise benefits, and complied with whole-of-government ICT policies and Treasury guidelines. The full business case could not be reviewed until the costs and benefits of contracting with suppliers were clear. The DCS assessed delivery confidence as medium, mainly due to several risks. These included the NSW Police Force adopting a new hybrid agile and waterfall delivery method as the systems integrator, difficulties faced by supplier B in travelling during the COVID-19 pandemic, and challenges in meeting the Australian Protective Security Policy Framework requirements when working with a foreign vendor.

This review expressed concern about the contract with supplier B, which set annual prices at a fixed rate until 2038, excluding any increases linked to the consumer price index (CPI) over the contract's lifetime. It advised that the IPOS program team should closely monitor the contract to ensure it did not discourage supplier B from acting as an innovative provider of modern software solutions. The review also suggested that the NSW Police Force should explore reward-sharing arrangements in future contracts with supplier B.

February 2021: Gate 4B review – Final tender evaluation

The aim of the review was to assess the solution and preferred option prior to committing funds, ensuring that the initiative would be delivered effectively and checking requirements against milestones.

The DCS rated delivery confidence as medium, concluding that the project could be successfully delivered if risks were addressed promptly. The review team emphasised the importance of implementing effective risk mitigation strategies when working with supplier B, a company that was relatively new and small but demonstrated growth and success. Additionally, the review team noted that the NSW Police Force was willing to take on more risk than previously.

December 2021: NSW Police Force internal audit health check

This review of the IPOS program focused on vision, leadership, risks and program management, and concluded that there were significant risks to longer-term program success. The report found that leadership of the IPOS program was driven by the Technology Command, and not led by the business, reducing the delivery focus on systems that directly supported operational policing. The review identified 4 areas that need urgent attention:

1. renewing and strengthening the basis for the business transformation
2. re-establishing strategic leadership of the program
3. aligning program governance with delivery focus
4. establishing independent program assurance.

The internal audit report noted that the chief information technology officer and the IPOS program director had both resigned, there were gaps in governance arrangements, and independent program assurance was lacking. The review team assessed the program as high risk.

September 2023: IPOS health check 2 review

The aim of the DCS health check 2 review was to assess whether the program was being managed effectively, and to identify risks and variations from the approach set out in the business case. The DCS rated delivery confidence as low, noting that the program was facing considerable uncertainty. This was largely due to a lack of essential elements, such as a detailed delivery plan, an overarching digital policing strategy, an updated business case and a robust operational execution model. The review recommended that the NSW Police Force appoint a single program sponsor, establish a delivery plan, and revise the business case and funding model for future needs.

September 2024: IPOS health check 2 review

This second health check review, conducted a year after the previous assessment, gave the program a medium rating for delivery confidence. The DCS found that leadership and governance structures had improved, and there had been some early positive outcomes in project delivery. Despite these advancements, the review highlighted ongoing challenges, including a lack of clarity around the program's scope, slow decision making, resourcing issues and difficulties managing complex interdependencies.

The review recommended further improvements in governance, risk management, organisational change management and financial oversight. The DCS also noted that there was no clear plan to replace the Computerised Operational Policing System (COPS) and advised the NSW Police Force to perform a comparative evaluation of low-code and police-specific commercial off-the-shelf solutions, using agreed criteria to reach a timely decision.

November 2025: PTP health check review

In November 2025, the DCS conducted a health check review of the PTP business case addendum. The review found that the program had made progress, with leadership, governance structures and delivery outcomes all showing improvement.

The review assessed the program against 5 key scope areas, rating both the current phase and readiness for the next phase as high. The review rated the delivery approach and risk management as medium, while the business case and stakeholder engagement received a low rating due to ongoing uncertainty over funding to complete the program. Overall, delivery confidence for the PTP was assessed as medium.

Appendix 4 – Status of PTP projects at December 2025







Projects already in production include BluLink, the Covert Operations Database (COD) – phase 1, mCOPS and mCOPS domestic violence, forensics and exhibits.



The NSW Police Force has also delivered improvements to data analytical capacity and underlying technology capabilities, such as systems integration.




Table 3 summarises the overall status of PTP projects at December 2025. The NSW Police Force presented project status reports to the monthly Police Technology Program (PTP) steering committee, using a red, amber, green coding approach. Projects that had not yet started or were being re-scoped were reported as grey.





The final column in Table 3 indicates whether the NSW Police Force expects to deliver this component of the PTP within existing capital funding.

Table 3: Status of PTP projects at December 2025

PTP program		Description and status at December 2025	PTP \$
Core policing solution		Computerised Operational Policing System (COPS) replacement.	partial
Phase 1		Crime recording and investigation management (including E@gle-i replacement). Expression of interest evaluation completed July 2025. Four vendors shortlisted. Prototype due end 2026.	yes
Phase 2		Information and intelligence management; procedural justice (including custody management); regulatory services, crime prevention, public safety. Completion June 2031.	no
Computer aided dispatch (CAD)		Next gen CAD. Status red due to delays in issuing contract. Forecast to go live November 2027 with release 2 forecast for October 2028.	yes
Forensics and exhibits		NEXUS (forensics register and minimum viable product for exhibits) live in February 2025. Well received by operational police. Project was red because the mobile version was delayed due to defects, with release expected in March 2026.	yes
Mobile futures – mCOPS		System to allow frontline officers to complete events and infringements in the field, reducing time at the station. Further development includes domestic and family violence module for mobile devices. Forecast completion June 2026. Project was amber because of delays and issues identified during testing.	yes
Mobile futures – Tempus		Digital notebook system. Proof of concept due February 2026. Project was amber because of delays.	yes
Mobile futures – Digital statements		Mobile application to allow officers to take statements in the field. Rollout planned for June 2026. Project was red because of delays.	yes

PTP program		Description and status at December 2025	PTP \$
Mainframe decommissioning		Mainframe hardware replaced July 2024, expected life 5 years. Mainframe decommissioning requires the NSW Police Force to implement core policing solution and remove legacy applications. In September 2025, project scope reduced to decommissioning 14 inactive applications, and 3 active applications added to the PTP business case. Status was grey because project manager had not yet been recruited.	yes
Core data and analytics services		Enterprise data and analytics capabilities, to remove data silos, improve data quality and deliver a single source of truth. Established as a separate project from the core policing solution in September 2025. The NSW Police Force planned to conduct a separate procurement process from February 2026.	yes

Enabling stream			
Integration platform and processes		Exchange of information between Integrated Police Operating System/PTP system and other NSW Police Force systems, plus with external agencies.	yes
Platform and security enablement		Cloud and network services, including support for mobile devices, encryption and monitoring system usage. Project was red due to delays in accessing system usage data from forensics and exhibits.	yes
Testing services		Standardised testing services to ensure quality, functionality and performance of new systems.	yes

Note:  indicates project not on track due to scope, timeline, budget or risks.  indicates project at risk.  indicates project on track.  indicates project not initiated or scope, timelines and budget under review.

Source: Audit Office of New South Wales review of NSW Police Force documents.

Appendix 5 – About the audit

Audit objective and criteria

This audit assessed whether the NSW Police Force has efficiently and effectively planned and sourced key components to upgrade technology systems that support core policing functions.

To address the audit objective, the following lines of inquiry and criteria were examined.

1. Did the NSW Police Force effectively plan for upgrades to technology to support core policing functions?
 - a) Planning processes were timely, informed by operational needs, and supported by robust business cases.
 - b) The NSW Police Force effectively managed changes in project budget, scope and timeframes, including responding to changes to technology.
 - c) The NSW Police Force considered the impact of legacy systems on the operational effectiveness of core policing functions.
2. Was the procurement of core policing technology systems transparent, competitive and compliant with NSW Government policies and procedures?
 - a) Procurement processes complied with NSW Government guidelines.
 - b) The NSW Police Force identified and managed conflicts of interest.
 - c) The NSW Police Force ensured that core policing technology contracts demonstrated value for money.
3. Did the NSW Police Force establish and maintain effective governance of core policing technology upgrades?
 - a) The NSW Police Force governance arrangements for core policing technology upgrades effectively supported the program.
 - b) The NSW Police Force effectively identified and responded to program risks and learnt lessons from previous attempts.
 - c) The NSW Police Force engaged staff and contractors with the required skills and experience to manage the project.

Audit scope, focus and exclusions

The scope and focus of the audit cover the following organisational activities:

- planning for technology upgrades, including project budgets, scope and timeframes
- procurement processes, such as short-listing, evaluation, due diligence and contract management
- project and program management arrangements
- governance structures and decision-making processes
- the impact of continued reliance on legacy systems on operational effectiveness.

The audit concentrated on activities from 2018 to December 2025, covering the integrated police operating system (IPOS) contract period and subsequent program activity.

The audit did not examine the ongoing management of business-as-usual information and communications technology (ICT) systems or question the merits of government policy objectives.

Audit approach

Our procedures included:

1. interviews with NSW Police Force staff responsible for ICT planning, project management, finance, procurement and operational use of core policing technology
2. observation of ICT systems used by operational staff
3. document review, including ICT strategies, requirements gathering, procurement records, contracts, project and program management materials, and governance documents such as decision logs and risk registers
4. review of business cases and gateway reviews
5. data analysis on project costs and expected benefits
6. consultation with relevant stakeholders.

The audit approach was complemented by quality assurance processes within the Audit Office of New South Wales to ensure compliance with professional standards.

Audit methodology

Our performance audit methodology is designed to satisfy Australian Auditing Standard ASAE 3500 Performance Engagements and other professional standards. The standards require the audit team to comply with relevant ethical requirements and plan and perform the audit to obtain reasonable assurance and draw a conclusion on the audit objective. Our processes have also been designed to comply with requirements specified in the *Government Sector Audit Act 1983* and the *Local Government Act 1993*.

Acknowledgements

The Audit Office gratefully acknowledges the cooperation of and assistance provided by staff at the NSW Police Force.

Audit cost

The estimated cost of the audit, including staff costs and overheads, is approximately \$352,000.

Appendix 6 – Performance auditing

What are performance audits?

Performance audits assess whether the activities of state or local government entities are being carried out effectively, economically, efficiently and in compliance with relevant laws.

The activities examined by a performance audit may include a government program, all or part of an audited entity, or more than one entity. A performance audit can also consider particular issues that affect the whole public sector and/or the whole local government sector. They cannot question the merits of government policy objectives.

The Auditor-General's mandate to undertake audits is set out in the *Government Sector Audit Act 1983* for state government entities, and in the *Local Government Act 1993* for local government entities. This mandate includes audit of non-government sector entities where these entities have received money or other resources (whether directly or indirectly) from, or on behalf of, a government entity for a particular purpose (follow-the-dollar).

Why do we conduct performance audits?

Performance audits provide independent assurance to the NSW Parliament and the public.

Through their recommendations, performance audits seek to improve the value for money the community receives from government services.

Performance audits are selected at the discretion of the Auditor-General, who seeks input from parliamentarians, state and local government entities, other interested stakeholders and Audit Office of New South Wales research.

How are performance audits selected?

When selecting and scoping topics, we aim to choose topics that reflect the interests of Parliament in holding the government to account. Performance audits are selected at the discretion of the Auditor-General based on our own research, suggestions from the public, and in consultation with parliamentarians, agency heads and key government stakeholders. Our 3-year performance audit program is published on the website and is reviewed annually to ensure it continues to address significant issues of interest to Parliament, aligns with government priorities and reflects contemporary thinking on public sector management. Our program is sufficiently flexible to allow us to respond readily to any emerging issues.

What happens during the phases of a performance audit?

Performance audits have 3 key phases: planning, fieldwork and report writing.

During the planning phase, the audit team develops an understanding of the audit topic and responsible entities and defines the objective and scope of the audit.

The planning phase also identifies the audit criteria. These are standards of performance against which the audited entity, program or activities are assessed. Criteria may be based on relevant legislation, internal policies and procedures, industry standards, best practice, government targets, benchmarks or published guidelines.

During the fieldwork phase, audit teams will require access to books, records or any documentation deemed necessary in the conduct of the audit, including confidential information that is either Cabinet information within the meaning of the *Government Information (Public Access) Act 2009* or information that could be subject to a claim of privilege by the state or a public official in a court of law. Confidential information will not be disclosed, unless authorised by the Auditor-General.

At the completion of fieldwork, the audit team meets with management representatives to discuss all significant matters arising from the audit. Following this, a draft performance audit report is prepared.

The audit team then meets with management representatives to check that facts presented in the draft report are accurate and to seek input into developing practical recommendations on areas of improvement.

A final report is then provided to the accountable authority of the audited entity(ies), which will be invited to formally respond to the report. If the audit includes a follow-the-dollar component, the final report will also be provided to the governing body of the relevant entity. The report presented to the NSW Parliament includes any response from the accountable authority of the audited entity. The relevant Minister and the Treasurer are also provided with a copy of the final report for state government entities. For local government entities, the Secretary of the Department of Planning and Environment, the Minister for Local Government and other responsible ministers will also be provided with a copy of the report. In performance audits that involve multiple entities, there may be responses from more than one audited entity or from a nominated coordinating entity.

Who checks to see if recommendations have been implemented?

After the report is presented to the NSW Parliament, it is usual for the entity's Audit and Risk Committee / Audit Risk and Improvement Committee to monitor progress with the implementation of recommendations.

In addition, it is the practice of NSW Parliament's Public Accounts Committee to conduct reviews or hold inquiries into matters raised in performance audit reports. The reviews and inquiries are usually held 12 months after the report received by the NSW Parliament. These reports are available on the NSW Parliament website.

Who audits the auditors?

Our performance audits are subject to internal and external quality reviews against relevant Australian standards.

The Public Accounts Committee appoints an independent reviewer to report on compliance with auditing practices and standards every 4 years. The reviewer's report is presented to the NSW Parliament and available on its website.

Periodic peer reviews by other audit offices test our activities against relevant standards and better practice.

Each audit is subject to internal review prior to its release.

Who pays for performance audits?

No fee is charged to entities for performance audits. Our performance audit services are funded by the NSW Parliament.

Further information and copies of reports

For further information, including copies of performance audit reports and a list of audits currently in-progress, please see our website www.audit.nsw.gov.au or contact us on 9275 7100.

OUR VISION

Our insights inform and challenge government to improve outcomes for citizens.

OUR PURPOSE

To help Parliament hold government accountable for its use of public resources.

OUR VALUES

Pride in purpose
Curious and open-minded
Valuing people
Contagious integrity
Courage (even when it's uncomfortable)



Audit Office of New South Wales

Level 19, Darling Park Tower 2
201 Sussex Street
Sydney NSW 2000 Australia

t +61 2 9275 7100

mail@audit.nsw.gov.au

Office hours: 8.30 am–5.00 pm

audit.nsw.gov.au