



**Firearms Safety
and Education**
New Zealand

Working Arrangement

Authorised under section 315 of the Arms Act 2026

22 September 2026

Foreword

This Working Arrangement reflects the respectful and trust-based relationship between New Zealand Police and Firearms Safety and Education New Zealand. It recognises that each agency has distinct statutory responsibilities, but that the safety of the public, staff, licence holders, and affected individuals depends on both agencies working well together. The arrangement is built on a simple principle: separate accountability, coordinated action, and mutual confidence in each agency's role, judgement, and professionalism.

Part 1 gives practical effect to that relationship where operational safety, public safety, personal safety, regulatory risk, and policing risk intersect. It provides confidence that risks will be identified early, information will move lawfully and in time, handovers will be clear, and urgent safety matters will be escalated through the right pathway. It is designed to ensure that people are kept safe without blurring the respective responsibilities of Police and FSE.

Part 2 sets out how the agencies will work across the boundary between law enforcement and firearms regulation. It recognises that some matters will require Police capability, reach, secure facilities, or constabulary authority, while regulatory stewardship and decision-making remain with FSE. The arrangement therefore provides guidance and a clear path a disciplined way to use the right authority for the right task, including where Police provides regulatory support, acts under direct statutory authority, or performs a delegated function for the Arms Regulator.

Part 3 records how Police will support FSE as its host agency by providing the corporate and enabling services needed for FSE to operate from commencement as a high-quality, efficient, and credible regulator. These services provide continuity, capability, and assurance while preserving FSE's regulatory independence. Together, the three Parts describe a practical, legally robust, and collaborative model for keeping the firearms system safe, effective, and trusted.



Richard Chambers
**Commissioner of
New Zealand Police**



Kelvin Watson
**Chief Executive of Firearms
Safety and Education New
Zealand**

Authorisation

Agreement between the Commissioner of New Zealand Police and the Chief Executive of Firearms Safety and Education New Zealand on the Working Arrangement

Introduction

1. The Arms Act 2026 establishes Firearms Safety & Education New Zealand (FSE) as the firearms regulator, as an autonomous agency of New Zealand Police. FSE will be led by an independent Chief Executive, accountable to the responsible Minister and subject to independent oversight. The new legislation coming into force on 23 September 2026.
2. Section 315 of the Arms Act 2026 requires the Commissioner to provide the corporate services and support necessary to enable the Arms Regulator to perform or exercise its functions, duties, and powers, except to the extent that any variation is agreed between the Commissioner and the Chief Executive.
3. Section 315 further requires the Chief Executive and the Commissioner to agree on working arrangements between the Arms Regulator and the Police, and to co-operate and collaborate with each other for the purposes of the working arrangements. The working arrangements must, without limitation, set out the resources and administration support that the Commissioner will provide to the Arms Regulator and the estimated cost of that support.
4. This Working Arrangement comprises three parts and two schedules: Operational Services; Regulatory Services and Corporate Services Header Agreements plus an Operational and Regulatory Services Schedule and a Corporate Services Schedule.

Authorisation

This Working Arrangement has been agreed by the Commissioner of New Zealand Police and the Chief Executive of Firearms Safety and Education New Zealand.

 Richard Chambers Commissioner of New Zealand Police	 Kelvin Watson Chief Executive of Firearms Safety and Education New Zealand
Date: 22 September 2026	Date: 22 September 2026

Executive Summary	4
Introduction	6
Interpretation	9
PART 1: Operations Header Agreement	13
Safety Accountability and Oversight	21
Review of Operational and Regulatory Activity	30
Terms of reference for the Liaison Working Group	33
PART 2: Regulatory Services Header Agreement	40
Part 2A: Police-delievered Regulatory activity under direct Statutory Authority	48
Part 2B: Delegated Regulatory Services - Isolated Communities	53
Part 2B: Delegated Regulatory Services - Airport visitor and traveller services	56
Part 2C: Other Support for Arms Act Regulation - Secure storage facilities	60
Part 2C: Other Support for Arms Act Regulation - Front desk services where agreed	64
PART 3: Corporate Services Header Agreement	67
Review of Corporate and Regulatory Services (cost and delivery)	84
Part 3: Governance, Legal, Policy and Communications	88
Part 3: People and Culture	92
Part 3: Health and Safety	97
Part 3: Finance and annual budget services	100
Part 3: Costs for Regulatory Services and Corporate Services	106
Part 3: Corporate processes, ICT platforms and identity services	110
Part 3: Premises, Property and Fleet	117

Executive Summary

1. This Working Arrangement gives practical effect to the Arms Act 2026 relationship between Firearms Safety and Education New Zealand and New Zealand Police. It preserves the statutory separation between firearms regulation and policing while setting out how the agencies will lawfully cooperate and collaborate including where their responsibilities meet and with regard to the provision of services and other support and their costs, and processes for delegating regulatory functions to constables and providing business records in accordance with sections 315, 311(3) and 358(5). FSE remains accountable for regulatory stewardship, licensing, compliance, regulatory decisions, delegations, registry quality, and advice to the Minister Responsible for Firearms. Police remains accountable for policing, law enforcement, public-safety response, operational command, criminal investigations, prosecutions, Police conduct, and ordinary Police powers. The core operating principle is separate accountability with coordinated action.
2. The Working Arrangement is structured into three companion parts. Part 1 governs operational cooperation where regulatory, public-safety, and policing responsibilities intersect. Part 2 governs Police-delivered regulatory services and other support for Arms Act regulation, including the circumstances in which a Chief Executive delegation under section 311 is required. Part 3 governs corporate and enabling services Police provides in its host-agency capacity, including people, finance, ICT, property, procurement, communications, information management, health and safety support, costs, and review arrangements.
3. The Working Arrangement model recognises that firearms safety operates across connected regulatory and law-enforcement functions. The agencies remain separate decision-makers, but they must be able to cooperate where the same matter involves regulatory risk, public or personal safety risk, information access, operational escalation, custody or evidential issues, or handover between regulatory and Police pathways.
4. The arrangement is designed to support lawful authority to act under legislation, regulations, via delegation or by means of support provided under this working arrangement. Police staff have the authority to provide administrative regulatory support, have a local presence, carry out licensing verification, recording, secure handling, referral, or other agreed support where authorised. A Chief Executive delegation is required only where a constable is asked to perform or exercise a specific Arms Regulator function, duty, or power that is not otherwise conferred by statute or regulations.

5. Information sharing is similarly disciplined: access, use, and disclosure must be grounded in the Arms Act, the Information Sharing Agreement, a delegation, an approved access arrangement, the Privacy Act, or another applicable legal basis. The Working Arrangement describes how the agencies will share information lawfully, escalate risk, coordinate action, preserve decision rights, and keep records that show who acted, under what authority, and for what purpose. The Working Arrangement describes the legislative context for information sharing and notes the complementary Information Sharing Agreement (ISA) that seeks to enable safe, transparent and lawful information sharing between the FSE and Police.
6. For Day 1, the emphasis is continuity with clear boundaries. Existing Police systems, staff, premises, finance processes, ICT platforms, and corporate services will continue to support FSE where needed, but hosting arrangements do not transfer regulatory accountability to Police or give Police a general role in FSE's statutory decision-making. Costs, service ownership, information access, health and safety responsibilities, and escalation pathways should remain visible, evidenced, proportionate, and reviewable.
7. The Working Arrangement also recognises that health and safety obligations may overlap. Operational safety, public and personal safety, critical incidents, Police response, and IPCA-related pathways are managed through Part 1. Workplace health, safety, and wellbeing are managed through Part 3. Those pathways are coordinated where necessary, but they serve different accountability purposes and do not displace any statutory duties under the Health and Safety at Work Act 2015.

Introduction

8. The Arms Act 2026 establishes the Arms Regulator, led by its Chief Executive, and separates firearms regulatory stewardship from Police's ordinary law-enforcement, public-safety, and operational-command responsibilities. The Act also recognises that the firearms system cannot operate safely or effectively unless FSE and Police cooperate in practice. Firearms licensing, registry integrity, public-safety response, criminal offending, information sharing, secure handling, and operational handovers will often be connected, even though the agencies remain separately accountable for their own statutory functions and decisions.

Purpose and scope

9. This Working Arrangement records the arrangements agreed between the Commissioner of Police and the Chief Executive of the Arms Regulator for the purposes of the Arms Act. It explains how FSE and Police will cooperate and collaborate under section 315, including the resources and administrative support Police will provide to FSE and the estimated cost of that support. It also provides the framework for the Chief Executive's delegation of specified Chief Executive functions, duties, and powers to constables under section 311 where that is necessary to support the Arms Regulator, and for FSE to provide Police with access to business record information where required by the Act.

Structure of the Working Arrangement

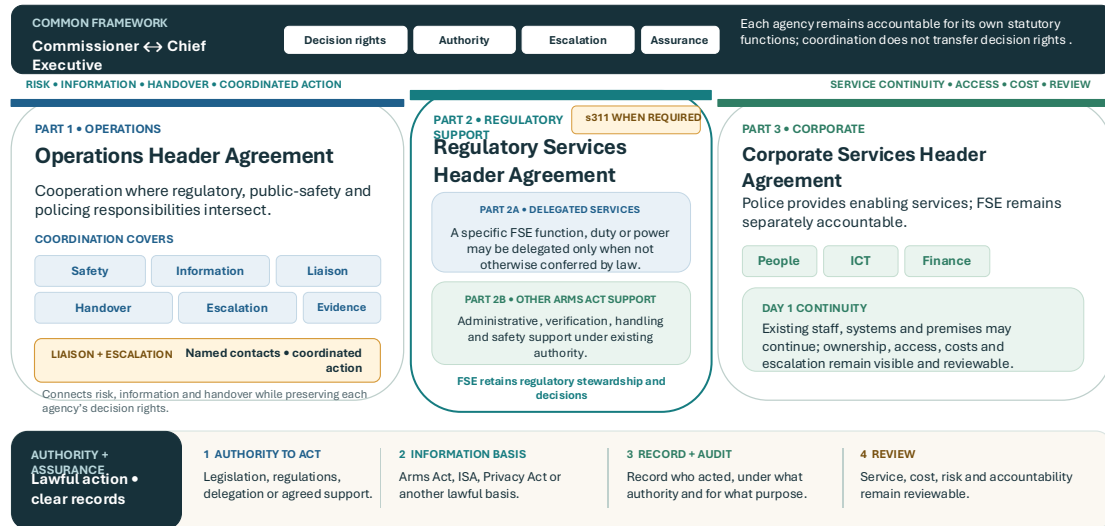
10. This Working Arrangement establishes the overarching framework for the relationship between FSE and Police under the Arms Act. It brings together the operational, regulatory-service, information-access, corporate-support, employment, and cost-allocation arrangements needed for Day 1 and for ongoing operation of the firearms regulatory system.
11. The Working Arrangement is structured into three complementary Header Agreements because there are three distinct systems of accountability, operations and service delivery involved:
 - **Operations Header Agreement (Part 1)** governs collaboration where FSE's regulatory responsibilities and Police's law-enforcement, public-safety, and operational-command responsibilities meet. It covers liaison, information-flow, handover, escalation, operational safety, operating models, and an overview of the information-sharing arrangements that support the Arms Act system.

- **Regulatory Services Header Agreement** has two parts. **Regulatory Services (Part 2A)** governs the process by which the Chief Executive may request specified regulatory support services to be delivered by Police constables whether because their involvement is permitted under the Arms Act or regulations, or under delegation from the Chief Executive, where the Chief Executive decides that delegation is necessary to support the Arms Regulator in performing or exercising its functions, duties, and powers. It preserves FSE's regulatory stewardship and decision-making. **Other Support for Arms Act Regulation (Part 2B)** covers additional or peripheral support services that support Arms Act regulation but do not require Police to perform or exercise Chief Executive powers, functions, or duties.
 - **Corporate Services Header Agreement (Part 3)** governs the administrative and enabling services Police provides in its host-agency capacity so FSE can operate as an organisation. It covers corporate services, people and culture, finance, ICT, property, procurement, communications, legal and policy support, information management, health and safety support, costs, service ownership, and review arrangements.
12. Each Header reflects a different relationship, legal context, delivery model, and accountability system. They therefore need separate scopes, authorities, responsibilities, service arrangements, cost treatment, and assurance mechanisms. However, the three Headers form a single integrated Working Arrangement and must be read and implemented together.
13. For review and escalation purposes, the Headers deliberately separate operational safety, regulatory-service delivery, and corporate service performance. Operational safety, information-flow, handover, public-safety, role-boundary, and regulatory/criminal interface issues are reviewed under Part 1. Delegation, service classification, service delivery, and authority-boundary issues for Police-delivered regulatory support are managed under Part 2A or Part 2B as applicable. Financial, purchasing, pricing, volume, affordability, cost-attribution, corporate-service, and host-agency performance issues are reviewed under Part 3.
14. The Headers are connected by a common principle: a person or agency must act under the authority that corresponds to the function being performed. Shared systems, services and operational cooperation do not transfer statutory decision rights or alter the respective accountabilities of FSE and Police.

15. Together, the three Headers provide a coherent framework for Day 1 and beyond. They define the relationship at the system level, while their associated schedules, operating models and service arrangements translate that framework into practical delivery.

Separate accountability with coordinated action

One firearms system • Working Arrangement under the Arms Act 2026



Capacity follows function, authority and purpose. Regulator staff may remain Police employees. Operational safety sits in Part 1; workplace H&S in Part 3.

Interpretation

16. In this Working Arrangement, references to **FSE** or the **Arms Regulator** are references to the statutory regulator or agency. References to **Regulator staff** are references to people assigned to, working for, or supporting FSE functions. Regulator staff may remain Police employees for employment purposes. References to **Police staff** are references to Police employees who are not Regulator staff. The capacity in which a person acts depends on the function being performed, the authority relied on, and the purpose of the activity.
17. The following terms used in this Agreement are further defined as follows:

Term	Definition
Arms Act	The Arms Act 2026.
Policing Act	The Policing Act 2008.
Firearm and arms item	Have the meanings given in the Arms Act.
FSE or Arms Regulator	The Arms Regulator established under section 303 of the Arms Act and known as Firearms Safety and Education New Zealand.
Police	New Zealand Police, continued as an instrument of the Crown under section 7 of the Policing Act.
Chief Executive	The chief executive of the Arms Regulator appointed under section 302 of the Arms Act.
Commissioner	The Commissioner of Police appointed under section 12 of the Policing Act.
Employment relationships and delegations	
Police employee	Has the meaning in section 4 of the Policing Act.
Commissioner employment delegations	A delegation by the Commissioner to the Chief Executive of specified employment-related powers, functions, or duties under the Policing Act for Regulator staff who report to the Chief Executive as part of FSE but do not have a Chief Executive delegation under section 311 of the Arms Act. The delegation enables the Chief Executive, or an appropriate delegate, to make employment-management decisions for those staff. It does not authorise the exercise of Arms Act regulatory powers.
Regulator staff	Police employees who report to the Chief Executive as part of FSE, while remaining Police employees for employment purposes under the Policing Act. Regulator staff include both: staff who have a written delegation from the Chief Executive under section 311 of the Arms Act to perform specified

	Arms Act functions, duties, or powers; and other FSE staff who do not require a section 311 delegation because they perform corporate, administrative, advisory, communications, official information, legal, or other support functions. For Regulator staff with section 311 delegations, section 309 of the Arms Act deems the Chief Executive to hold specified Commissioner employment powers under the Policing Act and removes the Commissioner's ability to exercise those powers for that group. For other Regulator staff, equivalent employment-management authority is provided through Commissioner employment delegations.
Police staff	Police employees, including constables, who are not Regulator staff. Police staff report to the Commissioner, and the Commissioner retains the employment powers, functions, and duties under the Policing Act for this group. Police staff may support FSE under this Working Arrangement, the Arms Act, associated regulations, or other lawful authority. This includes Police staff who provide administrative support or corporate services without exercising Arms Act regulatory powers, and constables who perform particular Arms Act regulatory functions where they are authorised directly by the Arms Act or associated regulations or have a written delegation from the Chief Executive under section 311.
Chief Executive delegation instrument	A written instrument made by the Chief Executive that authorises a person to perform specified Arms Act functions, duties, or powers on behalf of the Chief Executive, to the extent permitted by the Arms Act. The delegation instrument sets out the functions, duties, or powers delegated and any limits or conditions that apply.
Section 311 constable delegation	A written delegation by the Chief Executive under section 311 of the Arms Act to a person, including a Police employee who is a constable, authorising that person to perform or exercise specified Arms Regulator functions, duties, or powers on behalf of the Chief Executive for a particular case or class of cases, subject to any limits or conditions in the delegation. A section 311 delegation is required where the person is to make or exercise a delegated Arms Act regulatory decision, statutory power, or discretion on behalf of the Chief Executive. It is not required for administrative support tasks, corporate services, or functions that Police staff or constables are already authorised or required to perform directly under the Arms Act, associated regulations, the Policing Act, or other lawful authority.
Employment decision-maker	The person who makes employment-management decisions for a group of Police employees, including decisions about allowances, performance, disciplinary processes, personal grievances, Employment Relations Authority proceedings, settlements, special leave, pay in lieu of notice, compensation, ex gratia payments, and similar matters. For Regulator staff, this is the Chief Executive or an appropriate delegate, either under section 309 of the Arms Act or Commissioner employment delegations. For Police staff who are not Regulator staff, this is the Commissioner or an appropriate delegate.

Employment costs	The costs associated with employment processes, grievances, proceedings, settlements, or related civil claims. Unless otherwise agreed, employment costs sit with the agency whose decision-maker has responsibility for the relevant employment matter: the Chief Executive for Regulator staff, and the Commissioner for Police staff who are not Regulator staff. Police may still be named as a party to employment or civil proceedings because the staff remain Police employees.
No delegation required	No Chief Executive delegation is required where a task is administrative, corporate, logistical, advisory, communications, official information, legal, or other support work that does not involve making or exercising a delegated Arms Act regulatory decision, statutory power, or discretion. No Chief Executive delegation is also required where Police staff or constables are already authorised or required to act directly under the Arms Act, associated regulations, the Policing Act, or other lawful authority.
Information sharing and ICT	
FSE information	Information held by or for FSE, including information held in Police systems on FSE's behalf.
Police information	Information held by or for Police.
Information	Information in any form, including personal information, official information, classified information, confidential information, data, records, communications, images, intelligence, and system-held information.
Personal information	Has the meaning in section 7 of the Privacy Act 2020.
Official information	Has the meaning in section 2 of the Official Information Act 1982.
Direct data access	Approved electronic access by a user to information held in another party's system, without a separate case-by-case request, and subject to agreed access controls, use limits, audit, assurance, and other safeguards.
Service delivery model	
Part 1: Operational Services (including Police-led enforcement operations)	Cooperation, coordination, information sharing, liaison, escalation, and operating arrangements between FSE and Police where FSE's regulatory responsibilities intersect with Police's law-enforcement, public-safety, and operational responsibilities. Operational Services are governed by Part 1, the Operations Header Agreement. They include Police-led enforcement, investigation, response, public-safety, and related operational activity carried out by Police staff or constables under the Policing Act, the Arms Act, associated regulations, or other lawful authority. Operational Services do not include Chief Executive functions, duties, or powers that require a section 311 delegation unless a valid delegation has been made, and do not include administrative or corporate support services provided by Police to FSE.

Part 2: Regulatory Services (including Police-led enforcement of a regulatory nature or Police-led administration of a regulatory nature)	Police-led regulatory services comprise three categories. • First, directly authorised regulatory activity: functions, duties, or tasks that Police staff or constables are authorised or required to perform directly under the Arms Act, associated regulations, the Policing Act, or other lawful authority, without a delegation from the Chief Executive. This may include serving notices of suspension where the Act or regulations provide the authority. The Working Arrangement records how FSE and Police will coordinate this activity; it does not create the authority to perform it. • Second, delegated regulatory activity: Chief Executive functions, duties, or powers under the Arms Act that are delegated in writing under section 311 to Police staff or constables and performed for FSE in accordance with the relevant delegation instrument. This category applies where the person is to make or exercise a delegated Arms Act regulatory decision, statutory power, or discretion on behalf of the Chief Executive, and where direct statutory authority or administrative support is not sufficient. • Third, regulatory administration and support: administrative, processing, coordination, front counter, records, receipt, referral, verification, or other support provided by Police to FSE in connection with Arms Act functions. This category does not include making, recommending as decision-maker, or exercising a regulatory decision, statutory power, or discretion. It may include work performed by Police staff under this Working Arrangement and, where relevant, by Regulator staff who do not require a section 311 delegation.
Part 3: Corporate Services	Administrative and enabling services provided by Police in its host-agency capacity to support FSE as an organisation, including ICT, HR, corporate finance, property, fleet, procurement, security, accommodation, and other organisational support. Corporate Services are governed by Part 3, the Corporate Services Header Agreement.

PART 1: Operations Header Agreement

The operational framework for collaboration and cooperation

18. This Working Arrangement gives practical effect to the Arms Act section 315 by recognising that firearms safety operates across connected regulatory and policing functions. FSE is responsible for Arms Act stewardship and regulatory decision-making. Police is responsible for law enforcement, public-safety response and operational command. This Part establishes the liaison, information-flow, handover, escalation and operating-model mechanisms needed for both agencies to manage safety risks where those functions meet, while ensuring each person acts under the authority that matches the function being performed.

Purpose and scope of this agreement

19. This Working Arrangement – Operations Header Agreement records how New Zealand Police and FSE will work together under the Arms Act 2026 across distinct but connected statutory roles. It sets the enduring agency-to-agency framework for collaboration, cooperation, lawful information sharing, liaison, handover, escalation, stewardship, and operating models where the same firearm, person, premises, intelligence, or safety concern may engage both regulatory and policing functions.
20. Part 1 is limited to the operational relationship between Police and FSE. It does not set out the regulatory support services or corporate support services that Police may provide to FSE as purchased or hosted services. Those matters will be recorded in a separate Working Arrangement - Regulatory and Corporate Services Agreement document along with related schedules.
21. The operating models described in this document are the practical architecture for the Police - FSE operational law-enforcement and regulatory relationship. They support whole-system safety oversight, shared risk recognition, triage and assessment, intelligence connections, escalation and de-escalation, allocation of response and risk ownership, diversion-risk monitoring, visitor and border handovers, suspension and revocation implementation, and joint regulatory/criminal sequencing.
22. Information sharing underpins all operating models. Lawful, disciplined, and timely information flows are central to a mixed law-enforcement and regulatory operating environment. They are an operational capability needed to keep the public, staff, licence holders, and affected individuals safe while preserving clear statutory accountabilities. The information sharing and information access

pathways are summarised later in this section and explain how a combination of modes (including the Act and an information sharing agreement made under the Act) provides the permissions, purposes, safeguards, and practical pathways needed for the operating models to work together.

Operations safety and risk system

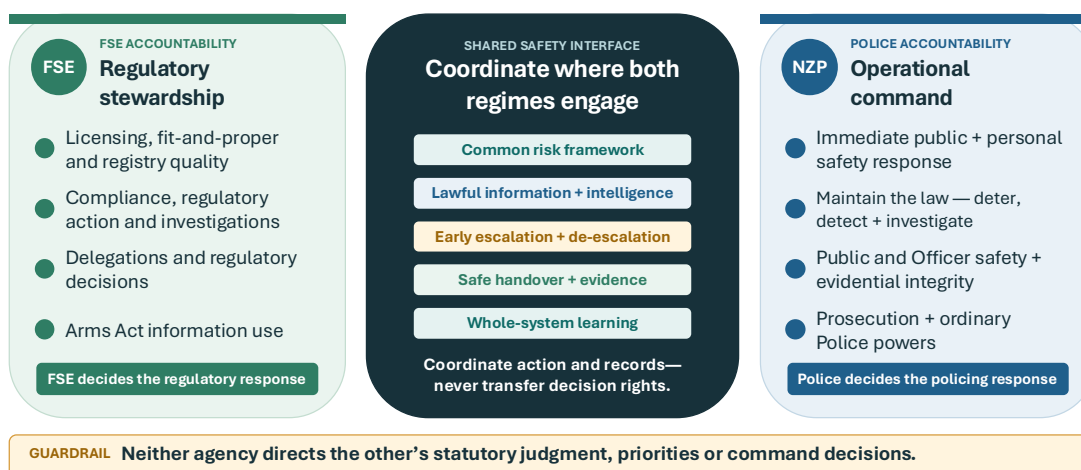
23. Because firearms safety depends on both regulatory decisions and law-enforcement action, the Working Arrangement needs shared objectives, clear responsibilities, reliable handover points, and performance information that supports oversight of the Arms Act system as a whole. The arrangement should not artificially separate regulatory and policing functions in operational settings where safety may depend on both agencies acting within their own authority.
24. The agencies will apply mutually reinforcing objectives that support public safety and harm reduction, effective regulation, coordinated whole-system safety, lawful information and technology capability, and a service-oriented regulatory culture. Those objectives include reducing diversion and proliferation of firearms, maintaining registry quality, preserving evidential integrity, managing safety-sensitive handovers, and ensuring regulatory and criminal matters do not fall between agencies.
25. Some matters will involve both regulatory and policing risk, such as credible threats, family violence risk, gang or organised crime risk, firearms offending, unsafe storage, or non-compliance that creates immediate danger, such as in situations where a licence holder's mental or physical health is impacting on their fit and proper status. In those situations, FSE manages the regulatory response and Police manages the immediate law-enforcement, public safety, and personal safety response.
26. This Working Arrangement sets the expectation of early escalation when a matter moves from ordinary regulatory administration into a safety concern, or when a policing matter creates regulatory consequences that FSE must consider. The escalation pathway should identify who controls any immediate incident, who owns the regulatory decision, what information must be shared, how firearms or records are handed over, and how both regulatory and policing decisions will be recorded.
27. The Operations Header provides the common framework for the Police - FSE operational relationship. It explains how two public agencies with different statutory roles will work together on shared safety risks, operational interfaces, information sharing, liaison, escalation, and the six operating models.

28. Firearms safety operates as one risk system across two statutory functions. FSE manages regulatory operational stewardship, licensing, compliance, regulatory decisions, delegations, regulatory investigations, registry quality, and Arms Act information use. Police manages law enforcement, public-safety response, operational command, officer safety, offence detection and deterrence, criminal investigations, prosecutions, evidential processes, and ordinary Police powers. Neither agency tasks or directs the other's statutory judgment, priorities, or command decisions.
29. Some operating settings are boundary-sensitive because the same facts may engage both regimes. These include armouries and other control points, recovered or surrendered firearms, visitor permitting and traveller movements, suspension and revocation service and retrieval, and matters where the same facts may support both a regulatory investigation and a criminal investigation. In those settings, the agencies will use agreed liaison, information-flow, handover, escalation, and operating-model mechanisms to manage safety risk without transferring decision rights.

WORKING ARRANGEMENT | OPERATIONAL HEADER

One firearms safety system, two statutory functions

Shared objectives and coordinated action connect the agencies; regulatory functions and Police functions remain separate.



3

Operating models maintain personal and public safety

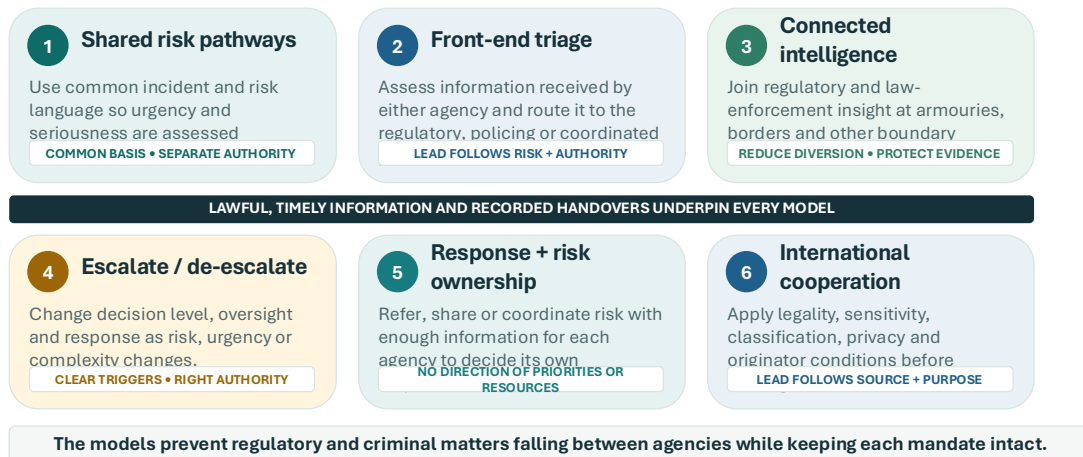
30. The operating models are the practical mechanism for connecting those functions when the same matter engages both regulatory risk and policing or public-safety risk. They explain how the agencies recognise and assess shared safety risk, connect intelligence, escalate and de-escalate concerns, allocate response and risk ownership, monitor diversion and registry-quality risks, and

manage international information sharing and cooperation. The operating models are outlined below.

WORKING ARRANGEMENT | OPERATIONAL HEADER

Six operating models connect regulatory and policing risk

Together they recognise shared risk, direct matters to the right pathway and preserve separate decision rights.



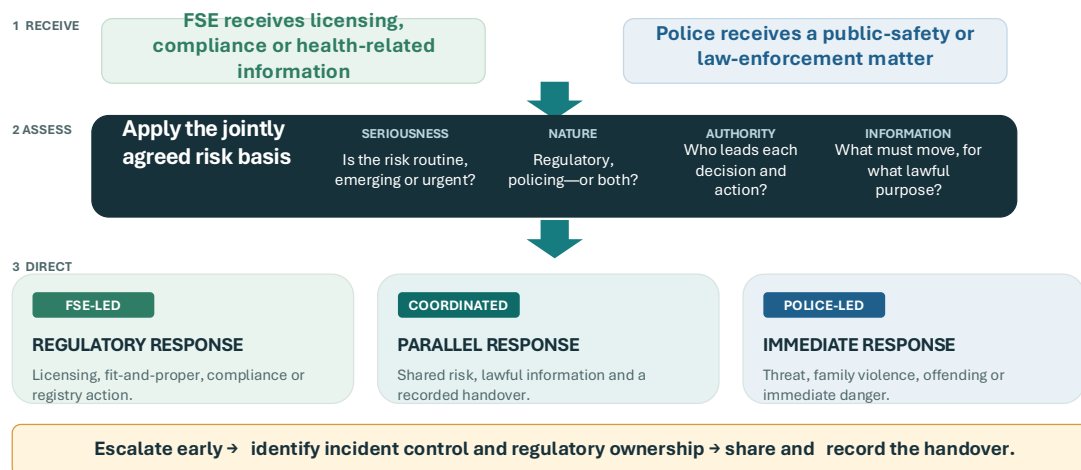
4

Model 1: Shared safety incident and risk information pathways

31. The first model establishes a shared understanding of safety risk. The two agencies will maintain a shared understanding of firearms-related risk so that the same information is not interpreted differently depending on which agency receives it first. A common risk framework helps the agencies recognise when a matter is routine, when it is becoming more serious, and when it needs urgent attention. This supports consistent decisions about who should lead, what information should be shared, and when a matter should be escalated.
32. This shared view of risk is also important for prioritising limited resources. It helps both agencies focus effort on the matters that present the greatest potential for harm, rather than on the matters that are simply most visible, easiest to action, or owned by the agency that received them first. It also makes capacity pressures more transparent, so that high-risk matters are not left unaddressed because responsibility is unclear or because each agency assumes the other will act.
33. In practice, this means the agencies can act earlier and more proportionately to keep people safe. Shared risk language supports timely triage, better escalation, and clearer handovers between regulatory and law enforcement responses. It also helps ensure that public safety, staff safety, and the safety of affected individuals are considered together, rather than separately through agency-specific processes.

Triage the risk at the front end

Health notifications, regulatory reports and Police incidents enter separately but use one agreed risk basis.



5

Model 2: Triage and assess risk at the front end

34. The Arms Act creates separate pathways for risk and incident information to be received by Police and by FSE. For example, the new legislation provides for FSE to receive, and own the response to, reports from health practitioners about licence holders' mental and physical health status. Information about a firearms-related safety risk may therefore enter the system through different channels, depending on whether it is first reported as a regulatory matter, a public safety concern, a health-related notification, or a law-enforcement incident.
35. Because the system needs to manage safety risk across both reporting streams, Police and FSE will agree an operating model for front-end triage and assessment. The model will set out how information received by either agency is assessed against a jointly agreed risk basis, how the seriousness and nature of the risk are identified, and how the matter is directed to the right regulatory, law-enforcement, or coordinated pathway.
36. The same operating model will guide information sharing between the two reporting streams. It should help determine when information needs to move between Police and FSE, the lawful purpose and role or function that supports sharing, and which information-sharing mechanism should be used. This allows the reporting systems to remain separate while still supporting a joined-up response to firearms safety risks.

Model 3: Connect intelligence for whole-system stewardship

37. The agencies operate within a shared intelligence ecosystem for the Arms Act. The Chief Executive's stewardship role requires visibility of the whole system, including regulatory intelligence, licensing and compliance trends, firearms and ammunition intelligence, regional and sector behaviour, emerging regulatory risks, and relevant law-enforcement intelligence held by Police. Police's focus remains law-enforcement intelligence, including offending patterns, criminal risk, operational safety, and investigative matters.
38. The intelligence functions remain distinct, but they need to connect. The Chief Executive needs enough system-level information to understand performance, identify emerging risks, and decide whether systemic regulatory action or system improvement is needed. Police need enough regulatory context to decide whether law-enforcement action, operational safety planning, or a coordinated response is required.
39. The agencies will maintain an intelligence operating model for boundary control points where firearms may move between lawful and unlawful contexts. This includes, for example, armouries, recovered illicit and lawfully held firearms, surrendered firearms, firearms held by businesses or licence holders, imports and exports, border or traveller pathways, and other points where firearms are received, validated, stored, transferred, released, seized, disposed of, or recorded.
40. The shared safety objective is to reduce diversion and proliferation of firearms in New Zealand. Diversion risk may arise through import and export pathways, grey or black-market movement through businesses or licence holders, theft, loss, unlawful possession, and firearms moving between lawful and unlawful contexts. Operating models should support both agencies to identify those risks, validate firearms against registry records, preserve evidence where required, and ensure information needed for regulatory or law-enforcement purposes is available to the right agency for the right purpose.

Model 4: Escalate and de-escalate as risk changes

41. The two agencies will liaise and cooperate on escalation and de-escalation governance and pathways so that the response can change as the risk changes. If a matter becomes more serious, urgent, or complex, there should be clear triggers for escalating it to the right decision-maker, forum, or agency lead. If the risk reduces, there should also be a clear way to step the matter down to a lower level of oversight, return it to routine management, or close it where no further action is needed.

- Clear escalation and de-escalation triggers, based on changes in risk, urgency, complexity, or operational safety;
 - Defined decision pathways so that matters move to the right level of authority, and can move back down when the risk has been managed or reduced;
 - Deciding how to coordinate regulatory and law enforcement resources and responsibilities where risk assessments indicate that both agencies should respond;
 - Structured forums for resolving high-risk issues, cross-agency ambiguity, or differences in prioritisation.
42. Suspension and revocation activity often sits at a safety-sensitive boundary. FSE may make, or be delegated to make, regulatory decisions about whether a person remains fit and proper or whether firearms should be surrendered. Police may also have powers to act in public-safety, personal-safety, or criminal-offending situations. The practical model must address who attends, serves notices, secures firearms, retrieves items, manages safety, records the handover, and owns follow-up in each case.

Model 5: Allocate response and risk ownership

43. The two agencies will agree how system risks may be transferred, shared, or referred across the regulatory and law enforcement roles. A transfer of risk does not mean that one agency can direct the other agency's priorities or resources. It means that, where one agency identifies that a matter is better managed through the other agency's statutory role, the matter is referred with enough information for the receiving agency to make its own decision about priority, response, and resourcing.
- Clear criteria for deciding whether a matter is best managed through a regulatory response, a law enforcement response, or a coordinated response;
 - Referral and handover processes that allow either agency to identify a system risk and ask the other agency to consider whether action is required within its own statutory role;
 - A shared way to identify and monitor cases that may fall into a gap because each agency has separately decided that the matter does not meet its threshold, priority, or available capacity for action.

44. This is particularly important where both regulatory and law enforcement investigative resources are scarce. Each agency will remain responsible for deciding how to allocate its own resources and prioritise its own effort. However, the agencies should use agreed risk criteria and liaison processes to make capacity pressures visible, identify matters where delay may create safety risk, and escalate cases where a lack of action by either agency could leave a material risk unmanaged.
45. Investigation activity is central to a functioning Arms Act regime. FSE needs the ability to undertake regulatory investigations, compliance assessment, audit, risk assessment, and graduated regulatory responses in relation to licence holders, dealers, ranges, clubs, storage, permits, endorsements, and other regulated activity. Police retains responsibility for criminal investigation, public-safety response, operational command, prosecutions, and the use of ordinary Police powers.
46. The boundary risk is that the same facts may support both a regulatory response and a criminal investigation. FSE will consider whether a proposed regulatory investigation could prejudice a Police investigation, prosecution, evidential process, or public-safety response. Police should also consider whether lower-level regulatory non-compliance is better managed through a proportionate and timely regulatory response. Both agencies should use liaison to identify the safest and most effective pathway, including where Police capacity, FSE regulatory risk, timing, evidence, disclosure, or delay creates an unmanaged safety risk.

Model 6: Manage international information sharing and cooperation

47. Police and FSE will agree an operating model for international information sharing, collaboration, and cooperation. The model will recognise that both agencies may receive or need to provide information through international law-enforcement, regulatory, border, customs, intelligence, or firearms-safety relationships, and that information received by one agency may be relevant to the statutory functions of the other.
48. The model should identify how Police and FSE will assess international information for relevance, legality, sensitivity, classification, originator conditions, privacy restrictions, national security implications, and operational safety. It should also distinguish between information that can be shared directly, information that requires the originating agency's consent before onward disclosure, and information that can only be summarised or used to trigger a separate domestic inquiry or risk assessment.

49. The model should support timely cooperation where international information affects firearms licensing, fit-and-proper assessment, border movements, import or export activity, transnational offending, organised crime, extremist or national security risk, unsafe firearms movements, or public safety concerns. It should also protect Police's international law-enforcement relationships and FSE's regulatory role by making clear who leads which part of the response, what information can be shared, what approvals are needed, and how decisions and handovers are recorded.

Safety accountability and oversight

External oversight and coordinated safety action

50. The operating models are also a safety-accountability framework. They show how FSE and Police will identify shared safety risks, exchange information lawfully, decide who should lead which response, hand matters over clearly, and record the authority used. These disciplines support public and personal safety and provide an evidential basis for later review if an incident, complaint, or oversight process occurs.
51. Section 317 provides for IPCA Act oversight, with any necessary modifications, where Arms Regulator functions, duties, or powers are performed or exercised. IPCA oversight may therefore apply to the Chief Executive, Regulator staff, and people acting under delegated authority when they are carrying out Arms Regulator functions, duties, or powers. Police also remains subject to its own IPCA accountabilities for policing conduct, public-safety response, operational command, use of Police powers, and related matters.

Interface with workplace health and safety

52. Where external safety accountabilities and workplace health and safety duties arise from the same facts, the pathways must be coordinated but kept distinct. IPCA oversight focuses on the conduct, authority, decision-making, and coordination of agencies and individuals performing Arms Regulator or Police functions. Workplace health and safety arrangements focus on duties to identify, manage, and learn from risks to workers and others affected by work. The same event may therefore require cooperation across both systems.
53. The effectiveness of the operating models will be relevant to both forms of accountability. If information is not shared when it should be, roles are unclear, handovers are not recorded, escalation pathways are not used, or responsibility for action is left unresolved, those issues may affect public safety, workplace

safety, and confidence in the Arms Act system. The agencies will therefore maintain the liaison, information-sharing, handover, escalation, review, and recordkeeping arrangements needed to show how Police and FSE cooperated while preserving their separate statutory responsibilities.

54. Nothing in this section transfers statutory accountability, regulatory decision-making responsibility, Police operational command, employment obligations, or workplace health and safety duties between the agencies. Where an incident engages both IPCA-related matters and workplace health and safety issues, each agency will meet the obligations that apply to it and coordinate with the other agency where required for notification, information provision, review, corrective action, and system learning.

Recognise dependencies and limits of agency control

55. Some matters referred to in this agreement sit outside the direct control of either agency and should be treated as external dependencies, assumptions, or matters requiring separate approval. However, the Liaison Working Group may identify, monitor, and escalate these dependencies where they affect operational safety, information sharing, role boundaries, accountability, or the effectiveness of the arms regime.

Information sharing and information access

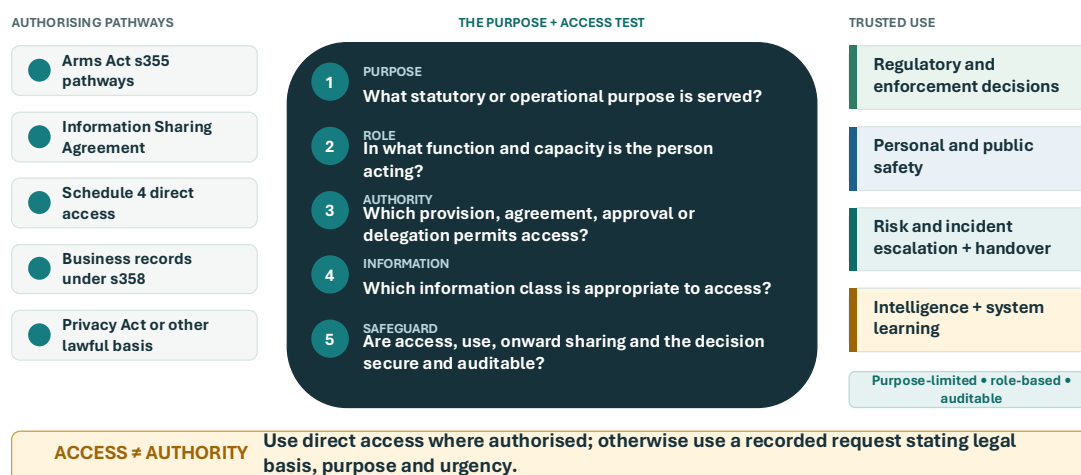
56. The Arms Act policy changes signal a shift toward greater transparency and greater certainty about what information is shared, what information may be accessed, and why that access is needed within the firearms regulatory and law-enforcement regime. The information-sharing system is therefore designed first as an operational and public-safety capability. Its guardrails are clear purposes, clear roles and functions, lawful access pathways, and transparent assurance over how information is accessed, used, disclosed and protected.
57. Lawful information access and sharing is a core capability for the Arms Act system. FSE and Police need timely access to relevant information so regulatory decisions, public safety responses, risk escalation, and whole-system learning are based on the right information at the right time. The purpose is not unrestricted access, but a clear and trusted system that supports safety by making the lawful purpose, authority, requesting role, receiving role, information class, access mechanism and safeguards visible before information is accessed or shared.
58. This is particularly important because firearms safety depends on information moving across regulatory and policing contexts when safety risk requires it.

FSE needs relevant Police-held information for fit-and-proper assessments, licensing, compliance, regulatory decisions, risk assessment and system stewardship. Police needs relevant FSE information for frontline and public safety and national security, incident response, offending detection, deterrence, prevention, and investigation and other lawful policing purposes. The arrangements are intended to support those lawful functions by making the relevant purpose, role, authority, and safeguard clear.

WORKING ARRANGEMENT | OPERATIONAL HEADER

Information sharing is an operational safety capability

The objective is timely lawful access—not unrestricted access or disconnected systems.



6

Authorising environment

59. The Arms Act enables transparency and provides assurance about what and how information is shared between FSE and Police. Information sharing between Police and FSE will occur through the following pathways:

- **Police access to arms registry information** - Police is entitled to arms registry information [section 355(1) of the Arms Act].
- **FSE access to Police information about holders/applicants** – FSE is entitled to information [section 355(2)] held by Police in relation to:
 - any applicant for a licence, approval, endorsement, permit, certification, or enrolment under the Act;
 - any licence holder, approved ammunition seller, shooting club, or shooting range;
 - that may assist the chief executive in the performance or exercise of the Arms Regulator's functions, duties, and powers under the Act.
- **Sharing by Arms Act agreement** – Additionally, information may be shared between FSE and Police under an agreement entered into

under section 355(3) of the Act and that has been consulted with the Privacy Commissioner [section 355(3)]. This information sharing agreement is published on both Police's and the FSE's websites.

- **An Order in Council** empower FSE to directly access law enforcement records including Police records, Land Transport New Zealand records and Corrections records under Schedule 4 of the Privacy Act. FSE access to Courts records is being addressed through a Memorandum of Understanding and through an Approved Information Sharing Agreement (in progress).
- **Licensed business records requested by Police** – FSE must provide Police with access to information held relating to the transactions and dealings of a licensed business. If FSE does not already hold the information required by Police, FSE must collect the required information from the licensed business and provide Police with access to that [s 358].
- **Other sharing as legally authorised elsewhere** – in addition to the above routes for sharing information, other legal modes of information sharing remain available, including Information Privacy Principle 11 and this other sharing will occur on a case-by-case basis, proactively or on request [section 355(5)].

Practical access and request pathways

60. Information sharing will occur by direct access where that is practicably possible and authorised for the relevant purpose. Where direct access is not practically possible, or where a request is required, communications will be made:
 - a. Through each party's designated contact point.
 - b. In writing using an agreed Request for Information form (RFI form) wherever possible, or if information is requested or received verbally in urgent cases, then a written record will be made of the outcome by the agency providing the information.
 - c. Specifying the legal basis that it is proposed the information could be released, the grounds in support, and whether the request is urgent or standard and the reasons for urgency.
61. Requests will be triaged having regard to the nature of the risk, the purpose for which the information is sought, the role and statutory functions of each agency, and the operational context in which the request is made. Each Party will respond as soon as reasonably practicable, having regard to the urgency of the

matter and the availability of relevant information, systems, and personnel. The different prioritisation categories are set out below:

Category	Description
Urgent	Required to support assessment or management of a serious or emerging safety risk.
Priority	Required to support a current operational or regulatory decision, but not an immediate public safety response.
Standard	Required for routine regulatory, assurance, administrative, or follow-up purposes.

62. Where an immediate public safety risk exists, Police retains responsibility for taking any immediate operational response available to it. FSE will support Police by providing relevant information or regulatory input as soon as reasonably practicable, within its operating model and available capability.

Information security, safeguards and assurance

63. All Police employees, including Regulator staff and Police staff, are subject to the Police Code of Conduct, including standards of integrity and requirements for protecting information and handling it only for legitimate work purposes. Failure by Police employees to comply with the Code may result in disciplinary action and/or IPCA investigation.
64. The Chief Executive will not permit anyone who is not a Police employee to directly access Police information. Information will only be disclosed to staff who need to see, or otherwise use the Information to achieve the purpose/s for which it has been supplied or accessed.
65. For the on-sharing of information, usual considerations will apply, including Information Privacy Principle 11 (or other lawful basis) when personal information is involved, or seeking permission from the other Party where other sensitivities arise. Any conditions that apply to the party that holds the information will also apply to the party that accesses or receives that information.
66. Each Party will take all reasonable steps to ensure Regulator staff and Police staff who are involved with the access or disclosure of Information are appropriately vetted, trained and cleared to the appropriate level of the Protective Security Requirements (PSR) classification system. This includes

staff who are responsible for submitting, receiving, assessing, and responding to Requests For Information (RFIs).

67. All Information will be managed in accordance with the New Zealand Government Information Classification System including the requirements set out in the Government's PSR, and the New Zealand Information Security Manual (NZISM).

68. Each Party will assign appropriate classifications and endorsements to each item of Information disclosed to the other Party.

69. A Party that receives Information will apply the mandatory safeguards and controls to ensure that information is sufficiently protected against any loss or unauthorised access, use, modification or disclosure, or any other misuse.

70. For Police held information that FSE receives or has access to, and which section 127 of the Arms Act applies to because disclosure would be likely to:

- a. endanger the safety of any person; or
- b. prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand; or
- c. prejudice the entrusting of information to the Police, the New Zealand Security Intelligence Service, or the Government Communications Security Bureau on a basis of confidence by:
 - i. the Government of any other country, or an agency of the Government of any other country; or
 - ii. any international organisation

The Chief Executive will ensure that such information is withheld in accordance with section 127 of the Arms Act, and where unsure, first consult with Police. Additionally, where a case involving such information is to be considered by the Firearms Licensing Review Committee under the Part 7, subpart 2 of the Arms Act, the Chief Executive will draw this to the attention of the Firearms Licensing Review Committee members and remind them of their confidentiality obligations and that the information is not to be released (sections 330 and 331 of the Arms Act refer).

71. The Parties also commit to adopting best practice personal information management practices to ensure that information accessed and shared is lawful, proportionate, purpose-limited, role-based, secure, and auditable, including:

- a. role based access controls to ensure staff only have access to required systems
- b. mandatory staff security and privacy training

- c. event logging, alerting and auditing
- d. software patching and updating
- e. systems certification and accreditation.

72. Police and FSE will agree timing and processes for review of direct access where approved, and handling of sensitive information, with controls that are purpose-limited, secure, and auditable where appropriate.

ICT repositories and lawful access

73. Police and FSE rely on connected ICT repositories and access arrangements to support lawful, timely and practical information use across firearms licensing, the Registry, compliance, vetting, public safety, intelligence connections, and whole-system stewardship. This section should be read with the Information Sharing Agreement and does not restate each permission, information class, safeguard, or review pathway.

74. The focus is the technology needed to find, access, interpret, update, correct, reconcile and use authorised information when needed, including repository access, system interfaces, access controls, reporting, audit logs, service dependencies, change management and data quality.

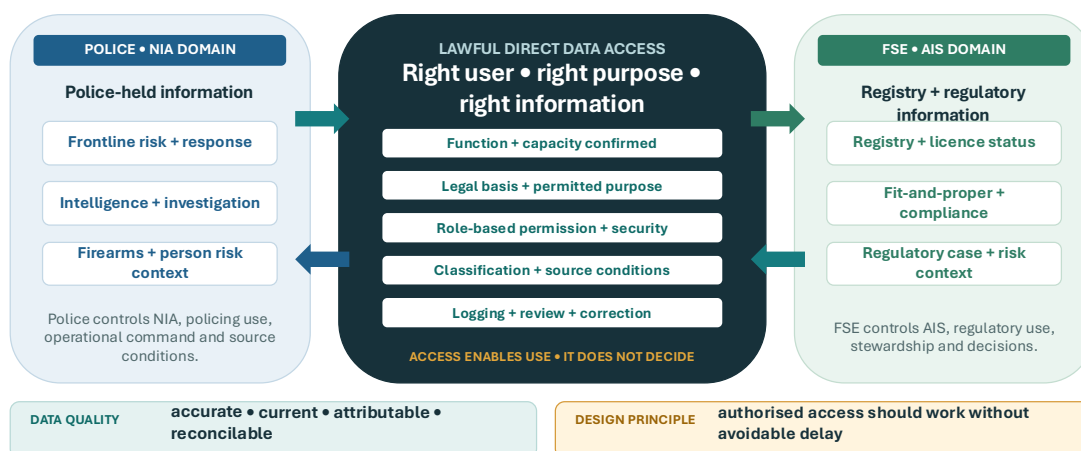
75. The agencies expect to use a mix of Police-managed systems, FSE-managed systems, shared interfaces, direct access, manual workarounds and vendor-supported applications while longer-term systems mature. Interim settings should preserve continuity, lawful access, data quality, auditability and safety without becoming the default model by accident.

Systems and access mechanisms

76. The systems and mechanisms covered by this section include, where relevant:
- AIS, the firearms registry, licensing, permit, endorsement, public-facing portal, case-management and regulatory workflow systems;
 - Police systems that hold or provide firearms-related information for frontline policing, risk assessment, intelligence, operational response, investigation, prosecution or public-safety purposes;
 - interfaces, access controls, system views, extracts, reporting tools, logs, data-matching, workflow queues and notifications that enable authorised access or exchange;
 - future system, integration, access-model and data-quality changes that may affect either agency's statutory functions.

Lawful direct access connects NIA and AIS

Authorised users reach safety-critical information without merging accountability; purpose, role, security and audit remain visible.



10

77. Where legislation or the Information Sharing Agreement authorises access to information for a specified purpose, technology settings should, using best endeavours, support that access in a secure, role-based, auditable and operationally usable way.
78. This section sets an expectation that future ICT design should apply the principle of best endeavours to enable lawful access. Where legislation or the Information Sharing Agreement authorises access to a class of information for a specified purpose, technology settings should support that access in a way that is secure, auditable, role-based, and operationally usable.

Data quality and accountability

79. A complete, accurate and timely firearms registry is a core safety and regulatory capability. FSE and Police will each keep the information they create, hold or rely on accurate, current, usable and available through the lawful pathways that apply.
80. For their respective responsibilities, the agencies will use best endeavours to:
 - keep firearms, licensing, permit, compliance, risk and safety information accurate, current and usable;
 - notify, correct and reconcile material information through agreed pathways; and
 - make data-quality, timeliness and access issues visible through liaison, ICT relationship management and review.

Roles, leads and shared flows

81. Lawful access depends on clear responsibilities for the systems, data, users and changes that affect each agency's work.
82. FSE is responsible for the regulatory and registry information, user needs, service requirements and access settings it needs for Arms Act functions, including the usability and quality of FSE-managed systems, workflows and vendor arrangements.
83. FSE is responsible for identifying the regulatory information, registry information, licensing information, including conditions on individual licences, compliance information, user needs, service requirements, and access settings it needs to perform its Arms Act functions. FSE is also responsible for ensuring that FSE-managed systems, vendors, workflows, and data-quality processes support lawful sharing, timely updates, auditability, and operational usability.
84. Police is responsible for the Police information, frontline-safety information, intelligence connections, access settings and system dependencies it needs for policing, public safety, detecting, deterrence, investigation, prosecution and enforcement functions.
85. Both agencies will identify named ICT and information-access leads to work with system, privacy, legal, security, data and business owners on access issues, data-quality issues and future changes.
86. For shared systems or information flows, the agencies should record the owner, users, purpose, authority, access process, correction process, escalation route, cost treatment, and change-notification approach.

Change management and review

87. Police and FSE will involve each other early in ICT, data, access, procurement, design and vendor-led changes that may materially affect lawful access, interoperability, registry completeness, data quality, safety, cost, timing or statutory performance.
88. Change proposals should identify the business reason, affected systems and information, access pathways, dependencies, timing, cost, privacy and security implications, service impacts and mitigations.

Day 1 priorities and review

89. From Day 1, interim ICT settings should preserve authorised, practical and timely access while system separation, replacement work, integration maturity and longer-term operating models develop.
90. Priority work should confirm the key systems and information flows, authorised access pathways, joint access matrix, known data-quality issues, and any changes needed to approvals, logs, guidance, training, review processes or the Information Sharing Agreement.
91. Review should test whether lawful access works in practice, information is accurate and timely, costs and dependencies are visible, and changes are being managed with both agencies' statutory interests in mind.

Review of operational and regulatory activity

Maintain the relationship, review the models, review information sharing and ICT access and escalate unresolved issues

92. Police and FSE will maintain the operational relationship through both structured and informal relationships. There are three connected levels for liaison: strategic leadership, operating model development through the Liaison Working Group, and day-to-day operational collaboration and cooperation. The Liaison Working Group (LWG) is the main mechanism for whole-system safety oversight at the operational boundary.
93. The LWG will own the development and maintenance of the six operating models. This includes keeping each model current, identifying practice issues, documenting lessons from operational cases, proposing changes, supporting staff understanding, and escalating unresolved policy, legal, resourcing, or operational issues to the right decision-makers. The detailed purpose, scope, chairing arrangements, recommendation-making role, membership, reporting, deliverables, and limits of the LWG are set out in Attachment A.
94. Overall, the liaison function will support practical case learning, agreed documentation, joint exercises or workshops where useful, regular reporting to strategic leadership, and oversight of the operating models and their effectiveness in delivering public and personal safety across the firearms regime. It should surface unmanaged safety risks, identify role-boundary ambiguity, test and maintain operating models, monitor recurring handover

issues, and escalate unresolved policy, legal, operational, or resourcing questions to the correct decision-makers.

95. The Parties agree that the liaison function does not replace statutory decision-makers, determine individual regulatory outcomes, direct Police operational command, or resolve individual investigations. Its role is to make the operational relationship work in practice: identifying dependencies, joining up the right people, tracking issues, clarifying priorities, supporting lawful information sharing, maintaining operating models, and ensuring unresolved matters move to the right forum.

Apply strategic leadership principles to protect the model and culture

96. Police and FSE will apply strategic leadership principles to maintain the statutory model, support constructive working relationships, and protect the cultural and behavioural shift required by the new regulatory arrangements.
 - a. **Respect for independent regulatory and law enforcement judgment:** leaders and staff will respect that FSE makes regulatory decisions under the Arms Act, even where those decisions are informed by Police information, operational advice, or public safety concerns.
 - b. **Constructive cooperation:** the agencies will work together in good faith, share relevant information through lawful pathways, and coordinate early where regulatory and law-enforcement responsibilities intersect.
 - c. **Early escalation of safety concerns:** safety risks, boundary issues, or matters moving from regulatory administration into policing or public safety response will be escalated promptly through agreed pathways.
 - d. **Clear role identity and service culture:** FSE leadership will support a service-oriented regulatory culture while maintaining clear role identity, so Regulator staff, Police staff, the public, Ministers, and partner agencies understand when FSE is acting as regulator, when Police is acting as Police, and when Police is providing agreed support to FSE.

Review, improve, and escalate through agreed pathways

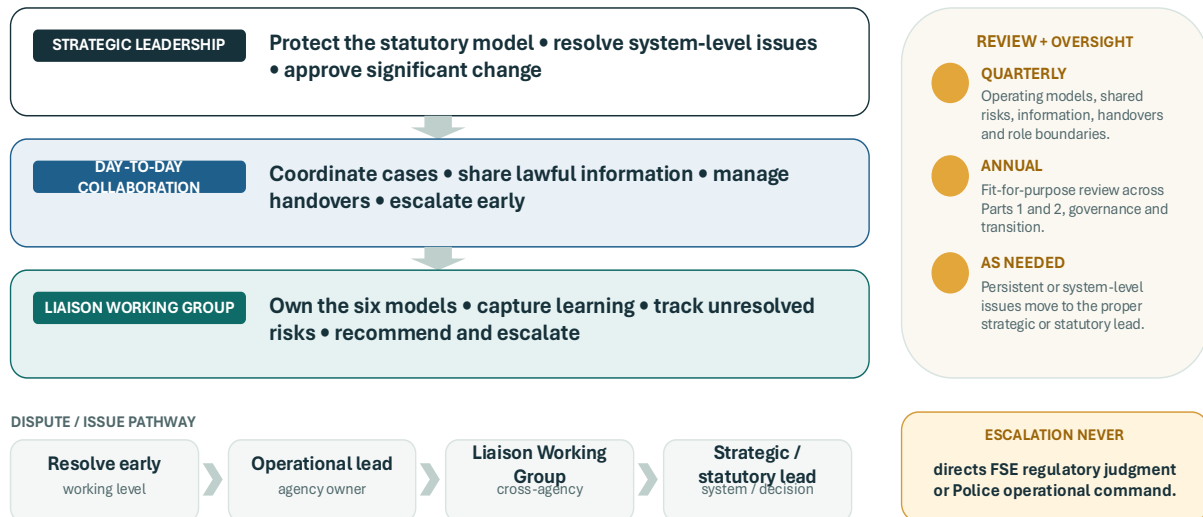
97. Representatives from Police and FSE will meet at least quarterly to assess and manage the successful operation of this Operations Header. The quarterly review will focus on the Police–FSE operational relationship, the six operating models, the liaison function, lawful information sharing, shared safety risks, escalation pathways, delegation and handover discipline, and any operational ambiguity affecting public safety or clear statutory accountability.
98. The review will identify issues early, agree practical improvements, manage dependencies, and ensure that the arrangement continues to support public

safety, effective law-enforcement and regulatory coordination, lawful information sharing, responsible use of public resources, and clear decision rights.

99. The review should expressly consider whether decision rights, information access, delegations, handovers, or accountability records or other processes where Police and FSE intersect are continuously improving or otherwise becoming unclear in practice. The purpose is to confirm that FSE remains accountable for regulatory stewardship and regulatory decisions, Police remains accountable for policing and law-enforcement response, and both agencies are maintaining the relationship capability needed for the model to operate credibly under scrutiny.
100. An annual review will consider whether this Operations Header (Part 1) and the Regulatory Services Header (Part 2), the liaison function, the six operating models, information-sharing settings, governance arrangements, relationship roles, and transition assumptions remain fit for purpose. The annual review will identify any changes needed to keep the operational relationship lawful, practical, clearly accountable, and focused on public safety.
101. An informal quarterly check will also consider operational safety issues arising from purchased Regulatory Services under Part 2 where those issues affect public safety, licence-holder safety, staff safety, information flows, handover into Police authority, escalation or de-escalation, role-boundary issues, or the effectiveness of the operating models. Financial, purchasing, price, volume, affordability, cost-attribution, service-standard, and service-provider performance issues for those services remain for review under Part 3.
102. Issues should be resolved at the lowest appropriate level first. Significant, persistent, unresolved, or system-level issues should be escalated through the agreed pathway to senior strategic leadership or the relevant statutory decision-maker. The pathway must not allow service, access, cost, performance, role-boundary, or accountability disputes to interfere with FSE's regulatory decisions or Police's operational command.

Three levels of liaison keep safety issues close to the work

Shared risks move through day-to-day collaboration, the Liaison Working Group and strategic leadership—without displacing statutory judgment.



7

Terms of Reference - Liaison Working Group

Defining the group's purpose

103. The Liaison Working Group is the joint Police - FSE forum that supports effective operation of the arms regime as a whole system. While Police and the FSE remain independently accountable for their respective statutory functions, powers and duties, including for personal, public and employment health and safety, the Arms Act expects the agencies to collaborate and cooperate. This Terms of Reference creates the formal structure for maintaining the practical collaboration, cooperation, liaison, information-flow, handover, escalation, and operating-model mechanisms needed for Police and FSE to manage safety risks at the operational boundary. The group supports shared stewardship of regulatory and criminal operations under the Arms Act through separate accountability with coordinated action, while preserving each agency's accountability for statutory functions, regulatory decisions, policing functions, operational command, employment obligations, and health and safety duties.

The Liaison Working Group maintains operating models

It joins practice, information and learning at the operational boundary, while formal decisions stay with the proper authority.



8

Set the group's role in whole-system oversight

104. Provide joint operational oversight of whether the collaboration, cooperation, liaison, information-sharing, and escalation mechanisms are working effectively across the arms regime as a whole system, while maintaining the principle of separate accountability with coordinated action.
105. Actively maintain the mechanisms that enable Police and FSE to work together in practice, including liaison contacts, escalation pathways, information provision, information access, lawful information sharing, issue resolution, operational learning, and continuous improvement.
106. Develop, test, document, and maintain the operating models between the law-enforcement and regulatory functions, including models for shared safety risk, triage and assessment, intelligence connections, escalation and de-escalation, allocation of response and risk ownership, international information sharing and cooperation, diversion and armoury control points, visitor permitting and traveller movements, suspension and revocation service and retrieval, and joint regulatory/criminal matters.
107. Identify operational ambiguity, role-boundary issues, handover issues, information-flow issues, diversion risks, registry-quality issues, custody or evidential questions, surge-capacity issues, regulatory/criminal sequencing issues, and unmanaged safety risks that may affect public safety, personal

safety, staff safety, clear regulatory decision-making, or effective law-enforcement response.

108. Recognise and preserve each agency's authority and accountability. FSE is accountable for licensing, compliance, regulatory decisions, delegations, lawful information use for Arms Act functions, and its own health and safety obligations. Police is accountable for policing, law enforcement, public safety response, operational command, officer safety, investigations, prosecutions, Police conduct, ordinary Police powers, employment obligations, and its own health and safety obligations. Parties agree they may have shared or overlapping health and safety, and shared public and personal safety accountabilities. Consultation, cooperation, coordination, liaison, information sharing, shared stewardship, or operational support does not transfer governance responsibility or statutory accountability between agencies.
109. Escalate unresolved legal, policy, privacy, security, resourcing, operational-command, regulatory-decision, regulatory/criminal sequencing, diversion, custody, evidential, border, traveller, service-and-retrieval, or system-performance issues to the appropriate decision-makers and report material issues to senior operational leadership in both agencies.
110. Initiate, coordinate, and liaise on reviews of information documentation, access and sharing arrangements where issues arise or where review is needed to support lawful, effective, and trusted operation of the arms regime. This may include reviews of information provision, direct access, role-based permissions, access logging, disclosure pathways, information-handling practice, suspected over-access or under-access, and lessons learned from incidents or operational cases.
111. Oversee only the operational safety interface with the Regulatory Services outlined in Part 2 of this agreement. The Liaison Working Group may review whether information created, received, documented, transferred, or relied on through Part 2 services is objective, accurate, complete, timely, and available through lawful pathways where that affects frontline operational decisions, FSE regulatory decisions, licence-holder safety, staff safety, public safety, handover into Police authority, escalation or de-escalation, or role-boundary issues. It does not review cost, price, purchasing, affordability, demand management, agreed service levels, or service-provider performance unless those matters create a material operational safety or role-boundary issue requiring escalation under Part 1.

Define the scope of the group's work

112. The Liaison Working Group will focus on the operational Police - FSE relationship as a whole-system safety interface. This includes shared safety risks, risk and incident triage, intelligence connections, escalation and de-escalation, allocation of response and risk ownership, international information sharing, operational information handling, diversion-risk monitoring, armoury and custody control points, visitor and traveller handovers, suspension and revocation service and retrieval, and joint criminal/regulatory matters. It will also monitor whether the mechanisms for collaboration and cooperation remain effective in practice, including whether information is moving lawfully and in time, whether handovers are clear, whether staff understand their authority, and whether unresolved risks are being escalated to the right level. The group will not manage purchased regulatory support services or corporate support services, except where a service issue creates an operational safety, information-sharing, role-boundary, or accountability issue that needs escalation.

Apply liaison operating principles

113. The following operating principles apply where public safety, personal safety, staff safety, regulatory risk, and policing risk overlap:
- a. **Safety first:** immediate risks to life, personal safety, officer safety, or public safety should be escalated to Police without delay, regardless of whether the issue is first identified by Regulator staff, Police staff, a delegate, or another authorised user, such as Customs New Zealand.
 - b. **Correct legal capacity:** each person must act under the authority that matches the function being performed at the time, including whether they are acting as Regulator staff, Police staff, a delegate, or another authorised user.
 - c. **Clear handover:** when a matter moves from regulatory management to policing response, the handover should be recorded.
 - d. **Purpose-limited information sharing:** information should be shared only where it is needed and lawful, but safety-critical information should not be withheld because of uncertainty about agency boundaries.
 - e. **Delegation discipline:** a constable performing a regulatory function must stay within the delegation and escalate regulatory matters outside scope.
 - f. **Oversight readiness:** records should be good enough to support Police review, regulator review, audit, complaints processes, and IPCA oversight where a critical incident occurs, including clear identification of the capacity in which Regulator staff, Police staff, delegates, or authorised users acted.
 - g. **Separate accountability with coordinated action:** the Liaison Working Group supports coordination, system learning, and shared

stewardship of regulatory and criminal operations under the Arms Act, but it does not transfer governance responsibility between agencies. FSE remains accountable for regulatory stewardship, regulatory decisions, delegations, lawful use of information for Arms Act functions, and its own health and safety obligations. Police remains accountable for policing, law enforcement, operational command, officer safety, public safety response, investigations, prosecutions, Police conduct, ordinary Police powers, employment obligations, and its own health and safety obligations. The group does not direct statutory judgment, determine individual regulatory outcomes, direct Police operational command, or decide the outcome of an individual investigation.

Set chairing arrangements and chair responsibilities

114. The Liaison Working Group will be co-chaired by nominated senior representatives from Police and FSE. Chairing of meetings will alternate between the Police chair and the FSE chair, unless the chairs agree a different approach for a particular meeting or issue.
115. Together, the two chairs will oversee the Liaison Working Group's work programme and support the day-to-day operational relationship between the agencies. This includes setting agendas, tracking progress against operating model development, ensuring issues are followed up, maintaining visibility of operational dependencies, and escalating matters that require senior operational leadership, statutory decision-making, resourcing, legal advice, or operational command.
116. The two chairs will meet quarterly to review progress, assess whether the collaboration and cooperation mechanisms are operating effectively, and consider whether the arms regime is operating as an effective whole system in line with the intent of the Arms Act. The quarterly chair review should consider operating model maturity, information flows, liaison effectiveness, unresolved risks, escalation patterns, role-boundary issues, lessons learned, and any recommendations for senior operational leadership in both agencies.

Recommendation-making

117. The two chairs may develop advice and recommendations for varying or amending the Working Arrangement: Operational Header Agreement. This may include recommending changes arising from operating model development, lessons learned, information-flow issues, role-boundary issues, escalation patterns, recommendations to policy and legislative stewards on changes in law or policy, changes in operational practice, or evidence that the collaboration and cooperation mechanisms are not operating as intended.

118. Advice and recommendations for variation or amendment should identify the issue, the proposed change, the reason for the change, any legal, privacy, security, operational, resourcing, or accountability implications, and the decision-maker or approval pathway required. The chairs may seek input from relevant subject-matter experts before making a recommendation.
119. The chairs may recommend changes, but they cannot themselves vary the Working Arrangement unless they have express authority to do so. Formal changes must be considered and approved through the agreed senior operational leadership or authorised decision-making pathway for both agencies.

Clarify decision rights and escalation limits

120. The Liaison Working Group may agree operational working practices, draft operating model content, issue registers, escalation recommendations, and continuous-improvement actions. It may not change statutory responsibilities, transfer governance responsibilities, direct Police operational command, direct FSE regulatory judgment, decide individual regulatory outcomes, decide the outcome of investigations, approve information sharing outside lawful authority, alter health and safety obligations, or commit either agency to resourcing or funding decisions. The group reports to senior operational leadership in both agencies and must escalate matters that require statutory judgment, operational command, formal legal advice, resourcing decisions, health and safety governance, or senior leadership direction.
121. Where an information access or sharing review identifies a need to change permissions, pathways, controls, technical access, legal authority, or the Section 356 information-sharing agreement, the Liaison Working Group may develop advice and escalation recommendations but must refer the matter to the relevant authorised decision-makers in each agency.

Confirm membership and expertise

122. Membership should include nominated operational, policy, legal, privacy, information-sharing, intelligence, implementation, and liaison representatives from Police and FSE. Members should have enough authority to identify issues, commit to practical follow-up within their area of responsibility, and escalate matters through their own agency where formal decisions are required. The group may invite subject-matter experts as needed, including representatives responsible for operational policy, direct data access, information security, international cooperation, frontline practice, or regulatory decision-making.

Set the group's operating rhythm

123. The group should meet regularly for the first six months from commencement, then move to monthly meetings as the six operating models mature. Urgent issues may be managed out of cycle where immediate public safety, staff safety, information-sharing, or operational-command issues arise.
124. The group should use early meetings after commencement to test Day 1 safety-critical interfaces, including armoury and diversion controls, airport and traveller surge arrangements, suspension and revocation service and retrieval, and regulatory/criminal investigation handovers. The purpose is to identify recurring information gaps, unclear decision points, operational capacity issues, registry-quality problems, custody or evidential questions, and any practice that could allow firearms to move out of lawful control.

Transitional liaison arrangements

125. A Day 1 liaison contact list, and escalation map will cover:
 - a. An initial work programme for developing the six operating models.
 - b. Interim practice notes for triage, escalation, handover, information sharing, and international information handling where needed.
 - c. A register of issues, risks, decisions, dependencies, and lessons learned.
 - d. Regular reporting to senior operational leadership in both agencies, including operating model maturity, whole-system operational effectiveness, information-flow issues, unresolved risks, role-boundary issues, escalations, lessons learned, and recommended changes.
 - e. Issues requiring formal decision, resourcing, legal interpretation, regulatory judgment, or operational command must be referred to the relevant senior operational leader or statutory decision-maker in the appropriate agency.

PART 2: Regulatory Services Header Agreement

Purpose of this Header

126. The Part 2 Regulatory Services Header governs Police-delivered support for Arms Act regulation. It sits within the wider Working Arrangement between FSE and Police and explains how Police support for Arms Act regulation is organised, scheduled, reviewed, and kept within clear authority and accountability boundaries.
127. The Regulatory Services Header Agreement and Operations Header Agreement are companion parts of the Working Arrangement. The Regulatory Services Header Agreement governs purchased, scheduled Police-delivered regulatory support services, including any delegated Arms Regulator function, duty, or power expressly identified in the Schedule.
128. This Header also explains what happens if safety or law-enforcement issues arise while Police is performing a Regulatory Service. Safety takes precedence. If a matter moves beyond regulatory support and requires public-safety response, criminal investigation, coercive powers, evidential handling, seizure, or Police operational command, the service must pause or hand over to the pathway in Part 1 and to the Police authority that applies. FSE remains responsible for the regulatory decision or follow-up, while Police remains responsible for the immediate safety and law-enforcement response.

Regulatory services scope

129. This Regulatory Services Header deals with Police-delivered support for Arms Act regulation. Consistent with the Interpretation section, that support is grouped into directly authorised regulatory activity, delegated regulatory activity, and regulatory administration and support. Part 2A covers directly authorised regulatory activity. Part 2B covers delegated regulatory activity. Part 2C covers Other Support for Arms Act regulation, including administrative, ancillary, or logistical support that does not involve performing or exercising an Arms Regulator function, duty, or power. The respective responsibilities for funding these services remain subject to further financial and funding analysis.
- a. **Part 2A: statutory-authorised regulatory activity** includes functions, duties, or tasks that Police staff or constables are authorised or required to perform directly under the Arms Act, associated regulations, the Policing Act, or other lawful authority, without a Chief Executive delegation. This includes frontline Police support for serving FSE-issued suspension notices and demanding, receiving, or securing arms items,

ammunition, restricted ammunition, and licence cards where the Act or regulations provide the authority, including where Search and Surveillance Act powers have been exercised.

- b. **Part 2B: delegated regulatory activity** covers Chief Executive functions, duties, or powers under the Arms Act that are delegated in writing under section 311 to Police staff or constables and performed for FSE in accordance with the relevant delegation instrument. This category applies only where direct statutory authority or administrative support is not sufficient, including limited, specified regulatory functions in remote or isolated communities, in international airport settings, or where assessed staff safety considerations mean Police support is necessary.
- c. **Part 2C: Other Support for Arms Act regulation** covers regulatory administration and support: administrative, processing, coordination, front counter, records, receipt, referral, verification, secure storage, or other ancillary support provided by Police to FSE in connection with Arms Act functions. This category does not include making or exercising a regulatory decision, statutory power, or discretion on behalf of the Chief Executive.

Review of Regulatory Services

130. The Regulatory Services Header does not create a separate review forum. Operational safety, information-flow, handover, public-safety, role-boundary, and delegation-boundary issues arising from Regulatory Services are reviewed under the Operations Header in Part 1, including through the Liaison Working Group and agreed operating models. Cost, resourcing, pricing, volume, affordability, and service-performance issues are managed through the Corporate Services Header in Part 3.

Schedules set out roles and responsibilities

131. The Schedules gives practical effect to this Header. A service will be described and scoped before it can be priced, scheduled, delegated, or reviewed. The Schedule identifies whether the activity is a Regulatory Service, Other Support for Arms Act Regulation, direct statutory or regulatory activity, administrative support, ordinary Police law-enforcement activity, or an FSE-only function.

Core operating principle: FSE decides, Police supports

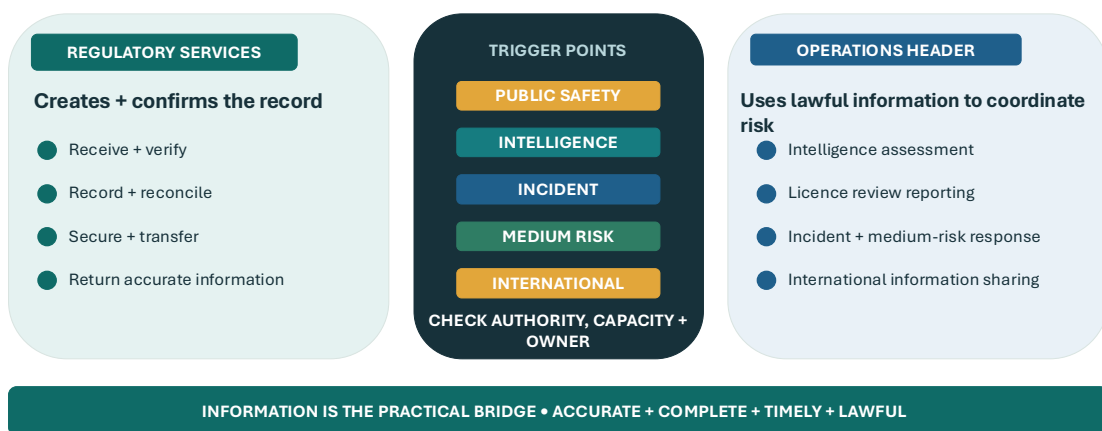
132. FSE remains the regulator and decision-maker for Arms Act regulatory functions. FSE is responsible for regulatory operations, regulatory records, and substantive regulatory decision-making under the Arms Act.

133. Police perform Other Support tasks unless a function, duty, or power is delegated or has been authorised by legislation. Police staff may issue temporary suspensions in some situations, but do not grant, refuse, suspend, revoke, cancel, impose conditions, exercise regulatory enforcement powers, or make other substantive regulatory judgements unless the relevant Arms Regulator function, duty, or power has either been lawfully delegated and is exercised within that delegation, or expressly provided for by legislation, such as for temporary licence suspensions. Information sharing and updates are key where Part 2 Regulatory Services are utilised.

WORKING ARRANGEMENT | REGULATORY SERVICES

Information connects service delivery and operations

A scheduled task may surface a Part 1 trigger while the service continues, pauses or hands over as the facts require.



Part 1 review covers safety, information flow and handovers; Part 3 review covers cost, volume, pricing and service performance.

20

134. The model uses Police capability without recreating the former combined firearms model. Police may perform Regulatory Services where lawfully authorised (by legislation or delegation) and Police has practical delivery capability, national reach, secure facilities, safe handling capability, district presence, or international airport touchpoints. The service role remains bounded by the Schedule, the authorising environment, and the distinction between regulatory support and ordinary Police law-enforcement activity.

Safety-risk and law-enforcement handover

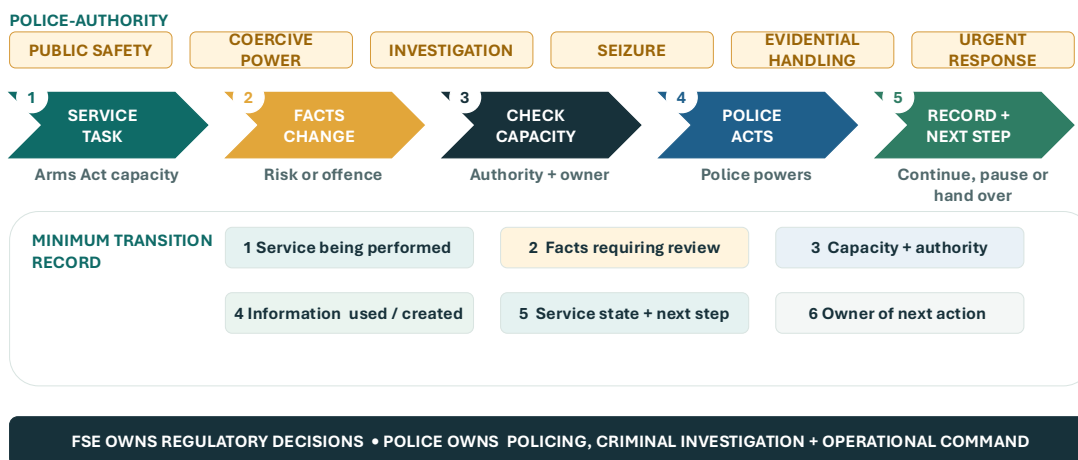
135. **Regulatory Services stop or pause when the facts require Police authority.** A purchased Regulatory Service may begin as other support, under a direct Arms Act or regulatory authority, or under an Arms Act delegation. If the circumstances move beyond routine regulatory support and require public safety escalation, coercive powers, criminal investigation, evidential handling, urgent response, or Police operational command, the matter moves outside the purchased Regulatory Service, and the relevant policing framework applies.

136. **The authority will match the facts.** An Arms Act delegation or legislative provision remains relevant to the specific regulatory task, but it is not intended to be used as a substitute for policing powers or as authority for tasks outside its scope. FSE retains responsibility for regulatory stewardship, regulatory decisions, Chief Executive-issued delegations, and regulatory records. Police remains responsible for ordinary Police law-enforcement activity, public safety response, constabulary powers, evidential handling, seizure using policing powers, officer safety, and Police operational command.

WORKING ARRANGEMENT | REGULATORY SERVICES

When facts change, check authority and ownership

If Police powers may be needed, record the acting capacity and whether the service continues, pauses or hands over.



21

Performance, assurance, and information quality

137. **Performance measures will protect both service delivery and regulatory independence.** Regulatory service performance should be assessed by whether Police-delivered support helps FSE carry out its statutory functions lawfully, consistently, safely, on time, within scope, and without blurring FSE regulatory decision-making or Police operational accountability.
138. **Information quality is a core service standard.** The Registry, FSE decision-makers, and frontline Police rely on complete, accurate, and up-to-date firearms information. Both FSE- and Police-delivered tasks must therefore ensure information and records in relation to actions taken are accurate, complete, timely, usable, and available through lawful pathways. Poor information quality or delay is both a delivery risk and a public safety risk.
139. **Assurance checks scope, authority, and quality.** Assurance for Regulatory Services should test whether each service is being delivered within the

Schedule, the correct authority, the agreed role boundary, the information-sharing pathway, the recording standard, and the pricing basis.

- a. availability, coverage, response times, escalation points, and priority rules;
- b. record quality, use of approved forms, guidance, and training;
- c. whether the task was correctly classified as Regulatory Services, FSE-only decision-making, ordinary Police activity, operational cooperation, or a corporate service; an
- d. whether any issue needs review under Part 1 for operational safety or authority-boundary reasons, or under Part 3 for cost, resourcing, or service-performance reasons.

Transition guidance for scheduled Regulatory Services

140. Some scheduled Regulatory Services are existing Police firearms activities being carried into the new model. The Day 1 task is to classify them clearly as Part 2A, Part 2B, or Part 3C, FSE-only, ordinary Police activity, or an operational interface issue.
141. That classification is especially important because Police staff need certainty before providing support for FSE, as to whether they are acting under statutory authority, under a Chief Executive delegation is needed, or providing other support; and when the matter has moved to Police law-enforcement, public-safety response, or operational command.

Part 2 does not create a separate review forum

142. **Operational-safety issues use Part 1.** Routine service issues should be managed by service owners and nominated points of contact. Where a Regulatory Service issue affects public safety, licence-holder safety, staff safety, information flows, handover into Police authority, escalation or de-escalation, operating model effectiveness, or role-boundary issues, it must be reviewed and escalated through the Operations Header Agreement in Part 1.
143. **Financial and corporate service issues use Part 3.** Issues about cost, demand, price, purchasing, affordability, cost attribution, agreed service levels, service standards, capacity, funding assumptions, cost recovery, or service-provider performance must be reviewed and escalated through the Corporate Services Header Agreement in Part 3.
144. **Issues engaging both pathways are coordinated, not merged.** Some issues may have both an operational-safety dimension and a financial or corporate service dimension. In those cases, the agencies should coordinate advice and

sequencing, while preserving the relevant decision rights and escalation route under Part 1 or Part 3.

Authorising environment Part 2A – Statutory authorisation

145. Part 2A covers Police-delivered regulatory services where Police, a constable, or another Police employee performs a regulatory function that is provided for in the Arms Act or regulations.
146. In the suspension context, Police constables may serve FSE-issued suspension notices, issue temporary suspension notices when Search and Surveillance Act powers have been exercised until FSE can make its own suspension decision, and demand and receive arms items that are subject to licence suspensions. Police staff, whether constables or not, may receive delivered arms items and related items, including under sections 139, 141, 143, and 145, and licence cards surrendered or delivered by licence holders at the end of a licence or when required to be produced, including under sections 121, 133, and 139. Police staff may also receive reports of lost, stolen, or destroyed arms items under section 136. Police Armourers engaged by the Regulator may lawfully possess arms items and provide expert advice under section 13(3)(viii). The regulatory decision remains with the Chief Executive or FSE decision-maker, while the Act and regulations may separately authorise Police involvement. For example, in an FSE-issued suspension context:
- FSE will decide whether to suspend a licence.
 - FSE may request that Police serve an FSE-issued suspension notice under the associated regulations because the licence holder is required by that notice to immediately surrender their arms items, ammunition, and any restricted ammunition in their possession to a Police employee.
 - Constables attending to serve the notice may demand that the arms items, ammunition, and restricted ammunition be surrendered to them because the notice and the Act provide that, on licence suspension, the person may be required to deliver those items to an Arms Officer or Police employee.

Authorising environment Part 2B – Delegated Regulatory Service

Constables may perform Arms Act functions and duties under delegation

147. A section 311 constable delegation is required where a constable is asked to perform or exercise a delegated Arms Act regulatory decision, statutory power, discretion, function, duty, or power on behalf of the Chief Executive, and that authority is not otherwise conferred on the constable by the Arms Act or

regulations. The need for a delegation is task-specific and depends on the authority required for the particular act. Section 311 also requires that, where a function is delegated to a constable by the Chief Executive, that delegation must be made in accordance with this Working Arrangement. For example:

- the provisions in the Act enabling inspection and approval of a licence applicant's secure storage (section 72(1)(b)) or inspection of licence holder security (for example, sections 75(1)(d) and (e), 88(3)(b), and 93(1)(b)) apply only to arms officers. Those activities are expressly specified as Arms Regulator functions.
- The decision whether to issue a firearms licence is a regulatory decision conferred on the Chief Executive under the Arms Act. Information collected through delegated regulatory activity may support that decision, but the decision remains with the Chief Executive or authorised FSE decision-maker.

148. In remote or isolated communities, or in situations of assessed staff safety risk, the Chief Executive may consider it necessary for a constable to perform specified delegated regulatory activity, such as an inspection or safe-storage check. In those circumstances, the Chief Executive may make a personal written section 311 constable delegation after first checking whether Police can assist and, if so, how the delegation should be addressed.

149. The delegation must be necessary to support the Arms Regulator, consistent with this Working Arrangement, and particular, bounded, and recorded. It should identify the function, duty, power, statutory decision, or discretion delegated; the delegate or class of delegates; the service context; scope; limits; duration; records required; escalation pathway; and any conditions needed to preserve FSE's regulatory accountability and Police's operational accountability.

Authorising environment – Part 2C Other Support for Arms Act Regulation

150. Part 2C covers elementary support for FSE's regulatory work where Police is not making the regulatory decision or exercising an Arms Regulator function, duty, or power.

151. That support may include limited front counter services (such as receipt of applications and other documents, appointment making and identity verification services). and arms items and ammunition storage services (Armoury Services).

152. For example, armoury or secure facility support may involve storing an item securely, recording custody and movement, enabling planned FSE access for registry verification, reporting discrepancies, or releasing the item on lawful FSE instruction.
153. If the task moves beyond ancillary support into notice service, seizure, detention, inspection, enforcement, evidential handling, public-safety response, or another authority-based activity, it should be managed under Part 2A or the relevant Police pathway.

Part 2A: Police-delivered regulatory activity under direct statutory authority

Purpose

154. This section covers Police-delivered regulatory activity that is directly authorised by the Arms Act or regulations. It includes Police-issued temporary suspensions, service of FSE-issued suspension notices, receipt of surrendered arms items, ammunition, restricted ammunition, licence cards and related items at suspension or licence end, and Police Armourer expert advice services.
155. FSE makes the regulatory decision. Where the regulations authorise Police to serve an FSE-issued suspension notice and the Regulator has required immediate surrender of arms items, ammunition, restricted ammunition, licence cards or related items, Police may serve the notice, require surrender where authorised, receive the items, and secure them.
156. No additional authorising instrument is required for tasks that the Arms Act or regulations already authorise Police staff or constables to perform. This includes serving suspension notices and demanding, receiving, or securing arms items, ammunition, restricted ammunition, licence cards or related items where those powers apply.
157. The model remains risk-based and directly authorised by legislation or regulations. FSE will need to serve other notice types itself unless a Part 2B section 311 delegation applies and may manage low-risk suspension notice service where Police attendance is not required.

Authority and role boundary

158. Police attendance should use the pathway that matches the Act or regulations, or ordinary Police authority for safety, criminal enforcement, evidence, seizure, investigation, or operational command.
159. FSE remains responsible for the regulatory decision and regulatory follow-up. Police remains responsible for the Police-led service and receipt of surrendered items, seizure (if powers need to be exercised), safety response, evidence handling, custody, and operational command where those matters arise.

160. Cost treatment for FSE-issued suspension notices service and arms item, licence, ammunition, and prohibited ammunition recovery will be dealt with through the agreed funding arrangements.

Serving FSE-issued suspension notices and receiving surrendered arms items (etc)

161. FSE makes the decision on whether to issue a suspension notice under section 146 or 147 of the Arms Act. A request by FSE for Police to serve an FSE-issued suspension notice and receive surrendered items will usually be processed as follows. The FSE Resolutions Team will create a 5G file for NIA and use Police iNET to enter a job, which will go to the relevant Police DCC for allocation at a local level and actioning.
162. Once service has been achieved, Police will complete a confirmation of service and, if any issues are encountered during service and surrender of the arms items etc, provide information about those issues to FSE and update the 5G matter in NIA. Where arms items, ammunition, or prohibited ammunition have been received, the items will be stored securely by Police (see Part 2C, Armoury services) and recorded in the PROP data repository.
163. In cases where FSE and Police have a shared interest and have been working together, for example where Police has an overlapping criminal investigation, FSE may send the suspension notice directly to the relevant officer in charge for coordinated service.
164. If the conditions are met and attending Police consider it appropriate, Police may resort to powers under the Search and Surveillance Act without further engagement with FSE, for example, to enter and search for illegally possessed arms items and ammunition.
165. The regulations allow low-risk suspension notices to be served by an Arms Officer, but Police will normally serve notices where risk or recovery considerations make Police attendance the safer or more practical pathway. FSE will not request Police to serve suspension notices where the Regulator does not require immediate surrender of arms items etc.

Receiving arms items, ammunition, restricted ammunition or licences under other statutory authority

166. Police may, by statute, receive arms items, ammunition, restricted ammunition or licences in a number of situations under the Arms Act in contexts that relate to a regulatory function.
167. If Police receives an item without prior notification from FSE, it will be recorded, stored and FSE notified. If FSE has required a person to deliver an item to a Police station, it will inform Police through the nominated operational contact points that the requirement has been made, and if Police receive those items, Police will record their receipt, store them, and notify FSE. The FSE will monitor items held by Police on FSE's behalf and regularly and promptly update Police as items need to be transferred or disposed of.
168. As described in the Operations Header, Police will notify or refer matters to FSE where Police identifies information that may warrant or other regulatory action. FSE and Police will coordinate where the same facts may support regulatory action, criminal investigation, prosecution, civil proceedings, evidential handling, safety response, or another legal pathway.

Expert Armourer services

169. Police have expert Armourers that provide services to Police under s 13(3)(vi) of the Arms Act. The FSE can also engage Police Armourer expert services for expert advice about samples of imported items; firearm modification and de-activation certification; advice, presentations, demonstrations, and training; technical on-site advice when large quantities of items are being uplifted, and other technical arms-related matters relevant to the exercise of regulatory functions under s 13(3)(viii) of the Arms Act.
170. Requests for sample inspection and reporting are to be made from the FSE Permits Team to the Police National Armoury. Requests for other Armourer advisory services are to be made on a case-by-case basis by FSE to the Police National Armoury Manager. An Armourer may also be required to give expert evidence in civil proceedings under the Arms Act (for example, where that evidence is relevant to a decision on a permit to import).

Limits and constraints

171. FSE remains responsible for regulatory decisions. Police service, arms item (etc) receipt, c, or safety action does not transfer that responsibility unless a function is directly authorised or lawfully delegated.
172. Police action must rely on the authority that applies: the Arms Act, and regulations, (and resorting to ordinary Police powers if required).
173. Records should show who acted, the authority used, any handover, custody status, and the next action owner.
174. Safety, enforcement, seizure, evidential, or operational-command issues must be escalated through the Police pathway. Regulatory follow-up remains with FSE.

Risks to law-enforcement/regulatory operations

- the main risk is role clarity: staff should be clear when a matter is an FSE regulatory decision, Police service or arms items (etc) surrender receipt, ordinary Police enforcement action, or a mixed matter requiring handover;
- handover and recording should confirm the authority used, custody or evidential status of any firearms or ammunition, registry or case-management update required, and the next action owner;
- cost treatment should remain visible where activity is FSE-requested, Police-led, or mixed; and
- early review should test whether any Day 1 workarounds remain necessary or should be updated through Part 1 or Part 3.

Controls and review points

175. For Day 1, controls should be simple and workable: clear tasking, basic recording, and a known escalation route as follows:
 - Tasking should identify the request, safety information, authority relied on, item or notice involved, contact points, and return information needed by FSE.
 - Records should capture the action taken, authority used, item status, handover, safety issue, and next action owner.
 - Interim guidance should cover only the essentials: who decides, who attends, what authority applies, when to stop, and who to call.

IN CONFIDENCE

- Early transition check-ins should focus on safety, timeliness, information quality, handover clarity, district consistency, and cost treatment.
- The first post-commencement review should decide what can remain light touch, what needs fuller guidance, and what should be escalated under Part 1 or Part 3.

Part 2B: Delegated regulatory services – isolated communities

Purpose

176. The FSE is normally expected to use its own staff to carry out its day-to-day regulatory functions. However, support may be requested on a case-by-case basis from constabulary staff who will be empowered by a Chief Executive delegation of specific regulatory functions on a case-by-case basis where a regulator function needs to be carried out.
177. A Chief Executive delegation is specifically required where a constable is asked to perform or exercise an Arms Regulator function, duty, or power that is not otherwise conferred on the constable by the Arms Act or regulations. The need for a delegation is therefore task-specific and depends on the authority required for the particular regulatory act. Additionally, section 311 requires that where a constable is to be delegated a function from the CE, that has to be done in accordance with this Working Arrangement.

Authorising environment

178. For each task that goes beyond lawful authority elsewhere described in the Working Arrangement, the delegation or authority should be kept task-specific. The tasking and outcome record should show the request, the delegation, the action taken, any information or item returned to FSE, any safety or enforcement issue, and the next action owner.

Isolated community regulatory services

179. The situations where the parties reasonably anticipate a delegation may be necessary are where a regulatory function needs to be delivered in an isolated community where FSE has no practical local (or proximate) presence. FSE remains responsible for regulatory judgement and decisions.
180. The regulatory functions that it is reasonably anticipated could need to be delegated in one of the above situations include:
- inspecting a licence applicant's or licence holder's secure storage (for example, ss 72(1)(b) 75(1)(d) and (e), 88(3)(b) and 93(1)(b)) apply only to arms officers.

- in-person interviews of applicants, referees, or other persons (including ex-spouses or partners) which will be relevant information for the decision whether to issue a firearms licence is a regulatory decision conferred on the Chief Executive under the Arms Act.
- serving some Arms Act notices (other than FSE-issued suspension notices which Police is expressly authorised to serve under the Regulations), for example, a notice revoking an endorsement where endorsed items need to be uplifted, or a notice revoking a licence when the person has become disqualified (section 153(1)) and in circumstances where there has been no prior suspension and therefore no earlier surrender of arms items (etc).

181. Where the CE considers that it is necessary to delegate a specified function for a specific case to a constable, the Chief Executive will first describe the anticipated scope of regulatory services to be delegated and other relevant information including location and provide that to Police. Police will confirm whether Police can assist in that particular case and, if so, how a delegation should be addressed. Then the Chief Executive may make a personal written Chief Executive delegation under section 311 and send that along with all other relevant information to the Police relationship manager who will create a file in NIA for the firearms activity, attach the documentation, and then forward it to the DCC for assigning to an officer.

Description of the service

- service (of documents other than suspension notices), security inspections, interviews in remote locations or risk to FSE staff safety;
- recording observations, including sighting firearms or storage arrangements, while referring any inspection findings to FSE;
- reporting back to FSE and escalating any matter that requires regulatory judgement, safety response, enforcement action, seizure, evidence handling, or Police operational command.

Risks to law-enforcement/regulatory operations

182. The main operational risk is role confusion. A Police officer in a remote area may be treated as the regulator even when the officer is only exercising a specific regulator function under delegation.

183. A further risk is that a planned support visit reveals unsafe possession, family harm indicators, threat, criminal activity, or other public-safety issues, requiring

Police to move into ordinary Police authority and FSE to retain any regulatory follow-up.

Risks to delivery

- Information accompanying FSE delegation requests may be too broad or unclear unless FSE tasking specifies what Police is being asked to do, and the delegation scope is sufficient for the task, what must be recorded or returned, and when staff should stop or escalate (and should not purport to limit normal Policing functions);
- unplanned or inconsistent district support may affect staff capacity, information quality, registry accuracy, service timeliness, or role clarity; and
- cost treatment may be unclear where an attendance begins as FSE-requested support but becomes ordinary Police safety, enforcement, evidence, seizure, or operational-command activity.

Controls and review points

184. For Day 1, FSE and Police should give targeted district tasking briefings for staff likely to perform this function. The briefing should cover the narrow local-support model, what FSE may request, the minimum recording required, what must be returned to FSE, and the stop or escalation triggers for safety, authority, enforcement, evidence, or regulatory-judgement issues.
185. The first review should test whether the Day 1 controls can remain light-touch, need fuller guidance or training, or require escalation under Part 1 for operational safety or Part 3 for resourcing, cost, or service-delivery issues.

Part 2B - Delegated regulatory services – airport visitor and traveller services

Purpose

186. The decision whether to issue a visitor licence and any associated permit to import is a regulatory decision conferred on the Chief Executive under the Arms Act.
187. It is anticipated that current practice around:
- (a) Police meeting visitor licence holders entering New Zealand; and
 - (b) Police facilitating pick-up of imported arms items travelling with a passenger into an international airport will continue, provided constables are delegated these functions by the Chief Executive.
188. Airport services are delivered at New Zealand international airports and involve printing and handover of a visitor licence and any associated permit to import documentation; checking licences and permits against arms items, ammunition, and related items arriving with the visitor or New Zealand firearms licence holder at entry to New Zealand; facilitating pick-up of imported items; and recording action taken, referral, and escalation where appropriate.
189. If the person is arriving other than by air and services need to be delivered by arrangement at another location, the services should be delivered by Regulator staff at an FSE office wherever possible. In that case, there would be no need for constabulary involvement. If that is not possible and the Chief Executive seeks to have the licence, permit, and arms items checked and noted by a constable, that should be specified to occur at a Police station or other location nominated by Police and pursuant to a delegation from the Chief Executive.
190. The agencies will distinguish traveller movements from commercial import and export activity. Commercial import and export generally involves cargo systems, external border processes, and separate agency arrangements, and should not be over-developed in this Working Arrangement unless another agency forms part of the agreed operating model.
191. FSE remains responsible for visitor permitting, licence-related regulatory decisions, permits, approvals, registry consequences, and other Arms Act decisions. Police supports agreed international airport touchpoints and remains responsible for airport safety, law-enforcement activity, and operational command.

192. Visitor permitting and traveller movements include interacting with both overseas visitor licence holders and New Zealand licence holders who are returning with firearms, ammunition, parts, or related items. Police's role will be specified in a section 311 delegation from the Chief Executive and limited to functions such as checking documents, confirming licence or permit status, sighting and recording items, validating information, referring matters to FSE, and escalating safety, unlawful, suspicious, urgent, or unresolved matters through the pathway that matches the authority required.
193. A Chief Executive delegation issued to the constable or group of constables under section 311 will be issued before relevant airport Police are asked to deliver the services for FSE. Where the Chief Executive considers it necessary to delegate specified functions to a constable or class of constables, the Chief Executive will first describe the anticipated scope of regulatory services to be delegated and other relevant information, including location, and provide that to Police. Police will confirm whether it can assist and, if so, how a delegation should be addressed. The Chief Executive may then make a personal written Chief Executive delegation under section 311.
194. The delegation agreed may be, for example:
- a. to a class of constables stationed or working at an international airport authorising the specified services for any/all visitor licence holders arriving at that site over a specified period of time, and/or other New Zealand licence holders arriving with arms items and related items; or
 - b. to a class of constables stationed or working at a particular Police station, describing specified functions or duties in relation to a specified visitor licence holder arriving by sea.
195. If the Chief Executive issues a delegation to airport Police in line with paragraph (a) above, FSE will send the delegation to the Police relationship manager for noting. Then, for each instance in which FSE seeks to engage that airport Police team for a visitor licence matter, FSE may email the relevant airport Police directly, providing both a copy of the delegation issued and relevant information required for the particular case.
196. If the Chief Executive issues a delegation to constables at a particular Police station in line with paragraph (b) above in relation to a particular visitor licence holder arriving by sea, FSE will forward that delegation, along with all other relevant information, to the [Police relationship manager], who will create a file in NIA for the firearms activity, attach the documentation, and then forward it to the DCC for assignment.

197. Ordinary Police authority continues to apply where the facts require public-safety response, law-enforcement activity, seizure (including under s 207 of the Arms Act), evidential handling, investigation, or Police operational command.

Authorising environment

198. A Chief Executive delegation will be issued to a constable or a class of constables. Ordinary Police authority will apply where safety, offending, seizure (including under s 207 of the Arms Act), evidence, or operational command issues arise.
199. For each involvement of a constable, the section 311 delegation must be issued. Regulatory decisions stay with FSE unless the function is directly authorised or lawfully delegated. Safety, unlawful possession, suspected offending, seizure, evidence, or urgent operational issues move to the Police pathway.

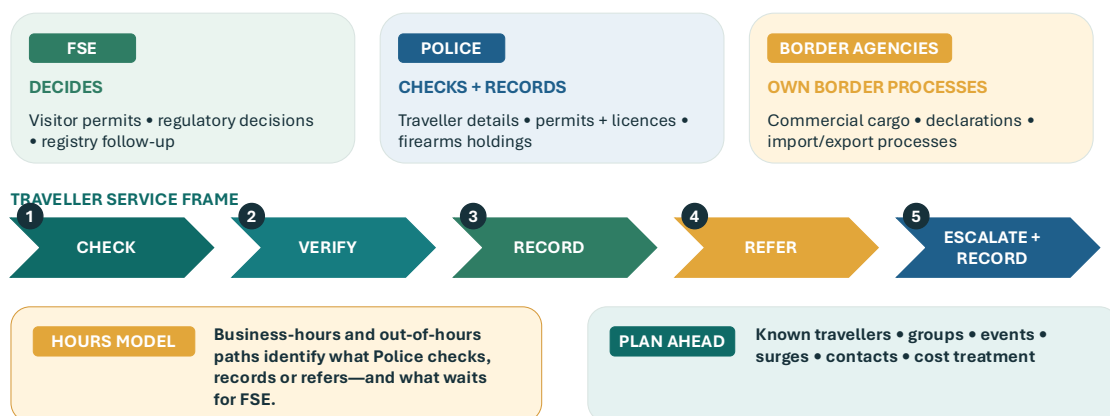
Description of the service

- Printing and handing over visitor licences and any associated permits to import; checking imported items against New Zealand firearms or visitor licences, approvals, permits, or other Arms Act documents. Tasks include sighting and recording firearms, ammunition, parts, or related items where needed;
- checking consistency between documents, declared items, visible items, registry information, and FSE or any relevant travel notifications;
- using FSE advance notice about travellers, groups, events, or travel patterns to support Police airport planning and escalation; and
- referring regulatory issues to FSE and safety, unlawful, suspicious, urgent, or unresolved matters to the right Police pathway.

WORKING ARRANGEMENT | REGULATORY SERVICES

Airport services centre on checking, recording and referral

Police checks traveller permits, licences and firearms holdings; FSE retains regulatory decisions.



Permissions, limits and constraints

200. Police may perform agreed airport and traveller checks where the task is authorised, safe, and clearly set out within Chief Executive delegations. This includes checking documents and traveller details, sighting and recording firearms or related items, validating information against approved systems or forms, and recording the outcome for registry validation, referral, follow-up, or assurance.
201. FSE remains responsible for visitor permitting, licence-related decisions, approvals, registry consequences, and regulatory follow-up.
202. The operating model must be clear about delegated functions and available FSE contact points for Police to engage with FSE if needed for referral or additional FSE regulatory decision-making.
203. If a traveller matter involves a discrepancy, unlawful possession, suspected offending, safety risk, seizure, evidence, or operational command, Police may pause the traveller service and move the matter to the pathway with the right authority.

Key risks

- role confusion at the airport, including uncertainty about when Police is providing checking, validation, recording, referral, or escalation support, and when a matter must move to FSE decision-making, ordinary Police authority, or another border-agency process;
- insufficient pre-notification of known travellers; increased traveller entry volumes or airport police duties impacting on Police ability to accept delegated functions.

Controls and review points

- For Day 1 delegations should be clear: agreed airport contact points, basic traveller check process, clear FSE referral routes, and a known Police escalation pathway.
- FSE should give Police early notice of known travellers, groups, events, or expected surges where practicable.
- An early transition review should focus on role clarity, traveller delays, information quality, surge demand, out-of-hours issues, referrals, and cost treatment including cooperation with other border agencies.

Part 2C: Other Support for Arms Act Regulation: Secure storage facilities

Purpose

204. Secure storage facilities service for arms items and ammunition when they are being held by Police for the Regulator is a key firearms control point. FSE needs regular, planned access to these firearms and related items held in those facilities so it can verify, reconcile, and trace firearms into the Registry, whether the items are lawfully held, surrendered, seized, recovered, illicit, unmarked, or otherwise unclear in status. The key requirement is that each item can be traced and explained through accurate records of its purpose, authority, custody status, location, access history, movement history, and next action owner.
205. Police may provide agreed district support, overflow or surge capacity, transport, secure custody, or specialist central armoury services where requested, authorised, scheduled, recorded, and costed. Physical separation is not required where recorded controls are safer or more workable, but both agencies must maintain enough visibility for registry reconciliation, diversion-risk monitoring, and lawful operational use.

Authorising environment

206. Secure storage facilities services operate under this Working Arrangement, the relevant schedule, section 315 support, (any they will have come into Police control through a direct Arms Act or regulatory authority or delegated function in another party), FSE and Police secure-storage, disposal, health and safety, hazardous-substances, and armoury procedures, Police safety and site-access requirements, and agreed PROP or other recording requirements.
207. For each stored item (or group of items), the record should identify the authority relied on. Routine receipt, storage, inventory, movement, supervised access, release on lawful instruction, disposal administration, and reporting back are usually Part 2B support. If the matter becomes evidence, public-safety custody, or Police operational activity, Police acts under the authority and process that applies to that purpose. Conversely, if Police have seized items under a policing power and then they no longer need to be retained for that policing purpose, but a Regulator can lawfully retain them under regulatory function (e.g. suspension or revocation), the parties will communicate and update the records relating to the stored items.

208. FSE access should be regular enough to support registry verification, reconciliation, correction, and track-and-trace work. Access must be planned, recorded, and managed under Police facility controls, including safety, security, supervision, site-access, safe-handling, ammunition and hazardous-substances controls, and any operational restrictions needed for the facility.
209. Both agencies should maintain a shared understanding of the policies and procedures that apply to each facility. Secure storage is not only an administrative control: it is a public safety and personal safety control because of diversion risk, a workplace health and safety control for staff and others who access the facility, and a hazardous-substances control where ammunition or other explosive material is stored or handled.
210. Records should identify where the item is held, why it is held, the authority relied on (and any changes to that while the item is being stored), custody status, relevant system record, FSE access, movement, testing, release, disposal, discrepancy, escalation decision, and next action owner.

Description of the service where agreed

- use of secure facilities as a joint law enforcement and regulatory capability, where agreed;
- receipt, storage, inventory, movement, release, disposal, and reporting for firearms, ammunition, parts, or related items held for FSE regulatory purposes.
- transport between agreed secure or disposal locations and to and from licence-holders;
- recording across FSE records, Police storage facility records, PROP where used, and providing information to FSE for registry;
- regular, planned FSE access for registry verification, reconciliation, correction, update, and track-and-trace work;
- clear identification of the purpose for which each item is held, supported by facility policies and procedures that manage diversion risk, staff safety, public and personal safety, and ammunition or hazardous-substances controls.

Secure capacity requires a clear custody purpose

Routine technical custody support usually needs no section 311 delegation; recorded purpose and authority distinguish each holding.



25

Permissions

211. Police may, where agreed and authorised:

- receive, store, record, move, release, or arrange disposal of items held for FSE regulatory purposes. Tasks include recording location, custody status, purpose, authority, movement, release, disposal, and completion status in the agreed system;
- provide regular, planned FSE access where needed for registry verification, reconciliation, correction, update, or track-and-trace work, subject to Police safety, security, site-access, supervision, safe-handling, and hazardous-substances requirements;
- apply and communicate the facility policies and procedures that govern secure storage, access, custody, handling, ammunition, hazardous substances, incident response, and escalation; and
- escalate suspicious, unsafe, unlawful, evidential, or public-safety matters into the relevant Police process.

Limits and constraints

- FSE access to Police armouries or lock-ups must follow agreed access, safety, security, supervision, handling, and incident-reporting requirements.
- If an item becomes evidence or is needed for criminal, coronial, public-safety, or Police operational purposes, it must move into the relevant Police process and be recorded accordingly.

- Inventory, ownership, serial number, condition, or legal-status discrepancies should be advised to each agency as appropriate.

Risks to law-enforcement/regulatory operations

- The main operational risk is unclear purpose, authority, custody status, or access history and incorrect retention. Each item must be capable of being traced and explained and disposal or transfer authorised as appropriate promptly by FSA.
- A further risk is diversion or proliferation if inventory, registry, movement, or evidential records do not align.

Risks to delivery

- Incomplete or inconsistent inventory and registry records;
- delay in notifying FSE of receipt, movement, release, disposal, or discrepancy;
- capacity pressure in secure facilities;
- unclear responsibility for overflow storage, transport, disposal, or destruction; and

Controls and review points

212. For Day 1, controls should be simple and visible:

- clear intake, recording, storage, access, reconciliation, release, movement, transfer, disposal, discrepancy, and custody-transfer steps.
- FSE access should be arranged where needed for registry verification, correction, reconciliation, and track-and-trace work.

213. The first post-commencement review should consider the public and personal safety, workplace health and safety, hazardous-substances policies and procedures, and access training needed for people to use or enter these facilities safely.

Part 2C: Other Support for Arms Act Regulation

Front desk services where agreed

Purpose

214. Front desk services provide elementary public-facing support for limited firearms-related regulatory matters where a Police station or front counter is the most accessible service point, or where Police-hosted premises are agreed as a practical location for receiving, checking, or referring firearms-related material. The service supports documentary receipt, inquiry referral to FSE, identity or document checks, and other agreed administrative touchpoints. It does not make Police front counters the regulator, create a general FSE service counter, or transfer FSE's regulatory decision-making role.
215. Police's role will usually be section 315 support: front-counter administration, document receipt and handover, referral of inquiries to FSE for response, verification and recording of identity for licence holders who have registered items electronically, and escalation. Where agreed, that support may be delivered from Police-hosted locations that can provide an appropriate public-facing touchpoint for FSE-related administration, with Police providing the premises, counter process, security, referral pathway, and recording support rather than assuming responsibility for the regulatory service or decision.

Authorising environment

216. Front desk services operate under this Working Arrangement, the Regulatory Services Schedule, approved FSE guidance, section 315 support, any direct Arms Act or regulatory authority, and ordinary Police authority where safety, offending, or investigation issues arise.
217. Routine receipt of documents, identity or document checks, referral, safe handover, and recording are Part 2C support. Inquiries and matters requiring FSE regulatory judgement will be referred to FSE. Threats, unlawful possession, suspected offending, seizure, urgent safety concerns, or matters with a criminal purpose move into the relevant Police pathway.
218. There is also an overlap with statutory enabled functions set out in Part 2A regarding the receipt of firearms and arms items. Some statutorily enabled functions from Part 2A may also occur in the front counter context, including:
- a. receiving surrendered, delivered, produced, or relinquished licences, arms items, ammunition, or restricted ammunition, including under sections 121, 133, 139, 141, 142, 143, 145, 159, 160, 161, 162, 163,

195, 343, 344, and 346, and including items that have not been required by the Chief Executive to be surrendered immediately upon suspension under section 146(5)(j) and (k) or section 147(3)(h) and (k);

- b. receiving reports of lost, stolen, or destroyed arms items under section 136; and
- c. receiving reports of bodily injury or death under section 276.

However, wherever possible, surrendered, delivered, produced, or relinquished arms items, ammunition, and prohibited ammunition should be prearranged with FSE and should occur at a Police station that has the appropriate level of firearms security.

Description of the service

- receiving documents, forms, applications, supporting material, surrendered firearms, ammunition, or related items where safe and agreed, and verifying identity or documents for FSE licensing purposes;
- providing a face-to-face service referral point where FSE is not immediately or locally available, such as providing FSE contact information or appointment booking with a FSE person or otherwise referring questions to FSE for direct response;
- escalating safety, unlawful possession, suspected offending, or urgent public-safety concerns through Police channels.

Permissions

219. Police may, where agreed, safe, and within the service schedule:

- receive documents, verify identity, receive firearms, ammunition, or related items;
- record the interaction, received items, referrals, and handovers;
- escalate threats, unlawful possession, suspicious conduct, or urgent safety concerns to FSE and/or Police.

Limits and constraints

- Firearms or ammunition may be received only where the counter is suitable, staff are prepared, safe-handling requirements are met;
- Police staff should be clear that they are not acting as an FSE service point for providing substantive information but rather as a referral or receipt point;

- Threat, unlawful possession, suspected offending, refusal, seizure, evidential issues, or urgent safety concerns must move to the Police pathway.

Risks to law-enforcement/regulatory operations

220. The main operational risk is role confusion: people may assume Police is the regulator because the contact point is a Police counter. A further risk is uneven capability across counters.
221. A key safety risk is a regulatory enquiry revealing threat, unlawful possession, suspected offending, or safety concerns that require Police action.

Risks to delivery

- documents, items, identity checks, or referrals not recorded accurately;
- delays in forwarding material or acknowledging receipt;
- inconsistent advice or service levels across locations;
- unclear which counters have an FSE Arms Officer available to provide FSE-capable service and which are referral-only, or emergency-only; and
- uncertain cost treatment for front counter services.

Controls and review points

222. For Day 1, controls should be simple: approved scripts, referral rules, basic receipt records, safe-handling steps, and a known escalation route:
- Minimum records should capture the person, item or document, action taken, time received, safety issue, referral, handover, and next action owner.
- Interim communications should make clear on the limited basis that Police is acting as an FSE referral point.

PART 3: Corporate Services Header Agreement

Introduction

223. This Corporate Services Header Agreement is part of the Working Arrangement under the Arms Act. It records the administrative and enabling services Police will provide so FSE can operate from commencement while performing its Arms Act functions through the authority, delegations, systems, and support arrangements that apply.
224. This Header should be read with the Corporate Services Schedule. The Schedule records the services provided, each agency's responsibilities, limits, request and approval pathways, escalation points, cost treatment, service owners, and matters that need further development after commencement.
225. This Header is one of three companion Headers. Part 1 governs operational cooperation where regulatory, public-safety, and policing responsibilities meet. Part 2 governs Police-delivered regulatory services and other support for Arms Act regulation. Part 3 governs the corporate services Police provides in its host-agency capacity, including people, finance, ICT, property, procurement, communications, information management, health and safety support, and related enabling services.

Purpose: corporate services

226. Corporate services are the systems, platforms, people processes, premises, assets, shared-service channels, specialist advice, and back-office support Police provides so FSE can operate from Day 1.
227. Corporate services are different from regulatory services. They support FSE as an organisation; they do not authorise Police to make FSE regulatory decisions or authorise FSE to exercise Police powers.
228. This Header keeps the practical boundaries visible: who owns the regulatory decision, who owns the employment relationship, who controls the system or asset, who holds financial accountability, and who is providing support.
229. The Day 1 employment and delegation position is a central feature of this Header. It is addressed in the next section and is not repeated here.

Delegation of employment powers, functions and duties from the Commissioner to the Chief Executive

230. Responsibility for certain employment powers, functions and duties in relation to FSE staff is intended to rest with the Chief Executive, rather than the Commissioner. Under the Arms Act 2026, there is a deemed statutory delegation which gives effect to this. The deemed statutory delegation only applies however to FSE staff who exercise regulator functions under a delegation from the Chief Executive and does not therefore cover all FSE staff. To address this gap in the legislation, the Commissioner has delegated responsibility to the Chief Executive for those same powers, functions and duties for all other FSE staff, by signing an instrument of delegation.
231. The deemed statutory delegation can only be amended or revoked through legislative change. While the instrument of delegation may be amended or revoked at any time, the Commissioner is committed to honouring the above intention and ensuring consistency across all FSE staff and will not therefore intervene unless and until exceptional circumstances arise (or the above gap in the legislation is fully and finally addressed through legislative change).
232. The instrument of delegation also confirms that responsibility for the applicable provisions of employment agreements and Police policies relevant to FSE staff whose positions are subject to any organisational redesign or change within FSE rests with the Chief Executive, rather than the Commissioner. This is for completeness, and to avoid doubt.

Each service has a clear authority and boundary

233. Each corporate service must identify the authority that allows it to be provided and the boundary of that authority. The authority may come from the Arms Act framework, ordinary employee authority, a financial delegation, an employment instrument, an information-sharing pathway, a system-access approval, a procurement or property arrangement, or another lawful permission.
234. Support authority is not regulatory authority. Police will provide HR, corporate finance, ICT, property, procurement, legal, communications, assurance, or other support without becoming responsible for FSE's regulatory judgements. If a matter requires a regulatory decision, it must be handled through the regulatory authority, delegation, or escalation path that applies to that decision.

Corporate service areas are grouped for accountability and review

235. The corporate services covered by this agreement and its schedules include:

- a. governance, policy, legal, communications and executive support;
- b. human resources, people capability, employment support (including recruitment)
- c. health and safety;
- d. Vote administration for the Arms Safety and Control output class
- e. finance, planning, accountability, audit, and performance information;
- f. ICT, cyber security, information management, privacy, and assurance;
- g. legal, policy, procurement, commercial, and contract support from time to time and by agreement; and
- h. property, premises, security, fleet, assets, risk, and assurance.

The Act identifies different sources of authority

236. This Working Arrangement identifies the capacity in which staff act when undertaking functions or tasks connected with the firearms regulator, as provided for in the Arms Act. Because authority and accountability differ depending on the task being performed, the same person may work within FSE, provide corporate or administrative support, exercise an Arms Regulator function, or act under ordinary Police powers. The purpose of this section, including the tables below, is to help identify, for each activity:
237. The pathways are explained to avoid treating employment status as the source of all authority. This Working Arrangement does not create the underlying powers, delegations, employment permissions, system-access approvals, or Police authorities. It records how the parties will identify the correct pathway, ensure the right people have the necessary authority to carry out a particular function or task, and preserve clear accountability for the relevant people, functions, tasks, roles, and responsibilities.

Table One

	GROUP 1: Regulator staff with delegations of Regulator Arms Act functions from CE	GROUP 2: Other Regulator staff working within FSE (no delegation)
Section 311 delegation from CE to this group	Yes	No
Examples of function of person working within FSE	Staff making decisions to issue licences and endorsements (and other things under the Arms Act), inspecting security, suspending and revoking firearms licences; and staff helping the Regulator “administer” the various Arm Act “regimes” (s 304, 308, 311).	Communications, OIA responses, legal advice, administration
CE relationship to this group (ability to exercise Policing Act employment functions)	CE deemed by Arms Act to have been delegated the following Commissioner’s powers, functions, and duties under the Policing Act (s 309(1)(a)): a. Section 18 (power to appoint) b. Section 58 (operate personnel policy consistent with good employer) c. Section 59 (must appoint on merit) d. Section 60 and 61 (must notify vacancies and appointments) e. Section 62 (review of appointments) f. Section 63 (may make acting appointments) g. Section 64 (may transfer employees internally) h. Section 65 (may temporarily assign, second locate internally) i. Section 70 (may suspend or remove) j. Sections 72-77 (provisions re compulsorily or voluntarily leaving Police due to incapacity)	In order for the CE to be able to exercise the same Policing Act functions employment-related functions listed at (a) to (j) in the previous column, the Commissioner will delegate those to the CE under s 310 of the Arms Act. This is similar to when the Commissioner delegates to Deputy Commissioners, and to Assistant Commissioner level.
Commissioner relationship to this group	Staff are still Police employees under the Policing Act, but Commissioner deemed by the Arms Act NOT to have the above functions, duties and powers in relation to this group of employees (s 309(1)(b)) – this means that the	Unlike the previous column, the Commissioner could legally still exercise those employment-related functions (i.e. intervene). However, the intention

IN CONFIDENCE

	Commissioner cannot intervene in or override a CE decision under one of the above provisions.	is that the CE will have and exercise the functions, duties and powers set out in s 309(1)(b) in relation to this group of employees.
Employment relationship problems/grievances/proceedings	CE (or appropriate delegate) is decision-maker in relation to any employment processes (e.g. payment of allowances, performance and disciplinary processes, responding to PGs, ERA proceedings, settlements) and is responsible for associated costs. Commissioner would be named as a party – the staff are still Police employees. <u>Associated decision making:</u> • <u>Decisions where there is no Police policy</u> – financial delegations will enable the CE to deal with these matters e.g. pay in lieu of notice, compensation, ex gratia payments, compassionate grants, • <u>Decisions where there is a Police policy</u> – this will be delegated to the CE by the Commissioner e.g. special leave, which is often used while proposal to suspend or dismiss.	While the delegation by the Commissioner does not affect the responsibility of the Commissioner for the actions of the CE acting under delegation (s 310(5)), the CE (or appropriate delegate) is decision-maker in relation to any employment processes (e.g. payment of allowances, performance and disciplinary processes, responding to PGs, ERA proceedings, settlements) and is responsible for associated costs. Commissioner would still be named as a party – the staff are still Police employees. <u>Associated decision making:</u> • <u>Decisions where there is no Police policy</u> – financial delegations will enable the CE to deal with these matters e.g. pay in lieu of notice, compensation, ex gratia payments, compassionate grants, • <u>Decisions where there is a Police policy</u> – this will be delegated to the CE by the Commissioner e.g. special leave, which is often used while proposal to suspend or dismiss.
Other civil claims or proceedings – e.g. HRRT, ERA (and beyond)	Commissioner would likely be named as a party – the staff are still Police employees. CE (or appropriate delegate) is decision-maker in relation to any of these and is responsible for associated costs.	Commissioner would likely be named as a party – the staff are still Police employees. CE (or appropriate delegate) is decision-maker in relation to any of these and is responsible for associated costs.
Financial delegations	The Commissioner will delegate the necessary financial decision making to the CE (s 310).	The Commissioner will delegate the necessary financial decision making to the CE (s 310).

Table Two

	GROUP 3: Police staff – constabulary with either statutory authority or CE delegations of Regulator Arms Act functions from CE or under the Arms Act	GROUP 4: Police staff (no delegation from CE) – could include constabulary
Section 311 delegation from CE to this group	Yes	No
Examples of function	Isolated communities; airport / visitor traveller regulatory functions	Administrative support and corporate services including front counter services (no regulator functions).
CE relationship to this group	CE retains responsibility for regulatory decisions only. CE does not have the Commissioner's powers, functions, and duties under the Policing Act as set out in s 309(1)(a).	CE retains responsibility for regulatory decisions only. CE does not have the Commissioner's powers, functions, and duties under the Policing Act as set out in s 309(1)(a).
Commissioner relationship to this group	Commissioner retains all employment powers, functions and duties under the Policing Act.	Commissioner retains all employment powers, functions and duties under the Policing Act.
Employment relationship problems/grievances/proceedings	Commissioner (or appropriate delegate) is decision-maker in relation to any employment processes (e.g. payment of allowances, performance and disciplinary processes, responding to PGs, ERA proceedings, settlements) and is responsible for associated costs.	Commissioner (or appropriate delegate) is decision-maker in relation to any employment processes (e.g. payment of allowances, performance and disciplinary processes, responding to PGs, ERA proceedings, settlements) and is responsible for associated costs.
Other civil claims or proceedings – e.g. HRRT, ERA (and beyond)	Commissioner (or appropriate delegate) is decision-maker in relation to any of these and is responsible for associated costs.	Commissioner (or appropriate delegate) is decision-maker in relation to any of these and is responsible for associated costs.
Financial delegations	Remain unchanged.	Remain unchanged.

Regulator functions

238. Regulator staff who perform or exercise Arms Regulator functions, duties, or powers do so under the authority of the Chief Executive, the Arms Act, regulations, or another lawful statutory basis. The Arms Regulator is established as an autonomous agency of Police. The Chief Executive is responsible for Arms Regulator functions and for the employment functions that apply to Regulator staff to the extent provided by the Arms Act or by an applicable Commissioner delegation.
239. Where a Regulator staff member requires authority to perform or exercise an Arms Regulator function, duty, or power, the authority must be identified and recorded. That authority may come directly from the Act or regulations, from a delegation by the Chief Executive, or from another statutory pathway. Regulator staff may remain Police employees for employment purposes, but their authority to perform Arms Act regulatory functions does not come from employment status alone.

Group 2. Regulator staff not performing Arms Regulator functions

240. Some Police employees may work within, be assigned to, or support FSE while performing corporate, administrative, or enabling functions rather than Arms Act functions, duties, or powers. For those functions, authority generally comes from the person's employment role, applicable Police or FSE corporate delegations, system-access approvals, financial or procurement authorities, and the support arrangements contemplated by the Arms Act and Policing Act.
241. These functions may include finance, human resources, information management, procurement, property, ICT, legal services, and other corporate support. A section 311 delegation is not required merely because a Police employee works in, is assigned to, or supports FSE. However, employment status and corporate authority do not, by themselves, authorise the person to exercise Arms Regulator statutory powers.

Group 3. Constables providing Arms Regulator functions

242. Some Arms Act functions are assigned directly by legislation or regulations to constables. In those circumstances, the constable derives authority directly from the relevant statutory provision and no section 311 delegation is required. Examples may include service of notices or other activities that Parliament or regulations have specifically allocated to constables because of operational safety, enforcement, or public-risk considerations.

243. In limited circumstances, where agreed between the Chief Executive and the Commissioner, a constable may perform or exercise an Arms Regulator function, duty, or power under a written delegation from the Chief Executive under section 311.
244. This pathway should be used only where delegation to a constable is necessary to support the Arms Regulator, all reasonable efforts have been made to enable Regulator staff to carry out the function or task, and the delegation is consistent with this Working Arrangement. Examples may include urgent operational situations or safety-related circumstances.
245. When acting under such a delegation, the constable acts only within the scope and limits of the delegated authority. The Chief Executive remains responsible for the decision to delegate and for the delegated regulatory function, while the Commissioner retains responsibility for employment functions for the constable.
246. Where legislation or regulation directly authorises the constable to act, no section 311 delegation is required. The constable acts under the authority granted by the relevant statutory provision.

Group 4: Police staff providing administrative or ancillary ‘Other Support’ for arms Regulation

247. Police staff may provide operational, logistical, corporate, or administrative support to FSE without exercising Arms Regulator statutory authority. Particular care is needed because constables may also hold ordinary Police powers or be directly authorised by the Arms Act or regulations for some arms-related regulatory functions. The relevant consideration is the function being performed and the authority required for that function.
248. Examples of administrative or ancillary Other Support may include:
- some administrative types of airport and visitor permit services;
 - some administrative types of front counter services;
 - armoury services such as the transfer, transport, storage, and custody of firearms;
 - identity verification activities;
 - information collection and recording;
 - other support associated with regulatory activity.
249. Where the activity is administrative or supportive in nature and does not involve performing or exercising an Arms Regulator function, duty, or power, no section

311 delegation is required. These activities are provided under the support arrangements contemplated by section 315 and described in the relevant service schedules. Where it is agreed that a constable is to perform an arms-related regulatory function for the Arms Regulator that is not otherwise directly provided for in the Arms Act or regulations, the constable must have an appropriate delegation or other lawful authority that meets any additional statutory requirements applying to constables.

Employment agreements and Day 1 transition

250. Employment matters for Regulator staff will continue to be managed through the employment framework that applies to Police employees, including the Policing Act, employment agreements, collective agreements, Police employment policies, Code of Conduct and any Commissioner employment delegation or other instrument that enables the Chief Executive or FSE managers to exercise agreed employment-related responsibilities. This Working Arrangement does not itself appoint staff, vary employment agreements, or confer hiring, dismissal, disciplinary, or remuneration authority.
251. As a practical transition matter, from 23 September 2026 existing Firearms Safety Authority staff, apart from constables or staff whose positions are otherwise disestablished, become Regulator staff and remain Police employees on their existing employment terms and conditions. They will report through FSE management arrangements to the Chief Executive. At or around commencement, the agencies will need to confirm the employment delegations or instruments needed for day-to-day people management, and the statutory delegations needed for staff performing Arms Regulator functions, and any other arrangements required between the Commissioner and Chief Executive.

Functional test

252. The functional test applies across all functions and tasks. The required authority depends on the nature of the activity being performed, not the employment status, position title, or organisational location of the person performing it.
253. If the activity involves performing or exercising an Arms Regulator function, duty, or power, a lawful statutory authority must exist, such as direct legislative or regulatory authority, a section 311 delegation, or another applicable statutory pathway. If the activity is administrative, corporate, logistical, or support activity only, it may generally be provided without a s 311 delegation provided it does not involve regulatory decision-making or the exercise of regulatory powers.

254. The word “employee” is used lawfully in the working arrangements, but the term is context-dependent. A person is a Police employee for employment law and payroll purposes while also performing work for Chief Executive of the FSE, supporting information sharing, or exercising a regulatory function under delegation. The legal issue is not whether the person can be called an employee; it is whether the document makes clear which capacity the person is acting in, which authority applies, and which agency is accountable for the decision or conduct in that context.
255. The working arrangement uses a permissive and functional framing. Staff may be described as Police employees where the employment relationship, pay, employment records, conduct processes, health and safety duties, or employment instruments are being discussed. They may be described as Regulator staff, staff supporting the Arms Regulator, or persons performing functions for the Arms Regulator where the context is regulatory delivery, service management, information handling, public-facing regulatory activity, or organisational accountability for FSE. Where a Police employee exercises a regulatory power or function under delegation, the drafting should identify then a delegation must be provided for the function being exercised, rather than relying only on employment status.

Terms and definitions

256. A distinctive feature of the arrangement is that Regulator staff operate in two legally connected but separate capacities. They remain Police employees for employment matters, including payroll, employment relations, conduct, benefits and health and safety, while exercising Arms Regulator functions under the statutory authority or delegation of the Chief Executive.

Human resources and employment roles and responsibilities

257. Police will provide the HR and employment services needed to support Regulator staff in the hosted model, including payroll, employment records, recruitment and onboarding support, position management, employee relations advice, health, safety and wellbeing support, learning administration, workforce reporting, and related people processes (including related frameworks and templates).
258. Police provides agreed workplace health, safety, and wellbeing systems and specialist support as part of the corporate services model. FSE remains responsible for identifying and managing risks arising from FSE-directed work, regulatory field activity, and the work of staff performing FSE functions, so far as those matters are within FSE’s influence and control. Police remains

responsible for risks arising from Police-directed work, Police workplaces, Police systems, Police operational activity, and Police staff. Where duties overlap, the agencies will consult, cooperate, and coordinate.

259. Nothing in this Working Arrangement limits, transfers, or excludes any duty owed by either agency, any officer, or any person under the Health and Safety at Work Act 2015 or any other applicable law.
260. Resources required to deliver the HR and employment services articulated in this document and the Corporate Services schedule will be New Zealand Police staff (or external providers as used by Police from time to time, at FSENZ's cost).
261. These services are provided as corporate support services and are bounded by the purpose for which they are provided. They do not give Police general decision-making authority over FSE's regulatory priorities, regulatory judgements, organisational culture, or day-to-day direction of regulatory work.
262. FSE remains responsible for setting workforce expectations, capability needs, role requirements, performance expectations in the regulatory environment, and the cultural direction of the autonomous regulator.
263. Police's processes, policies, and Code of Conduct will continue to apply to Regulator staff from Day 1. It is acknowledged that the Chief Executive may operate outside the strategic and policy framework of the New Zealand Police (s 307(7) of the Arms Act). However, the Chief Executive will advise the Commissioner of any proposed changes to Police's policies as they apply to Regulator staff and is solely responsible and liable for any such changes. Any changes will need to be clearly documented and communicated as applying to all Regulator staff.
264. Where Police HR staff or FSE Chief Executive support staff need access to employment records or sensitive people information to deliver these services, that access must be role-based, purpose-limited, proportionate, auditable, and consistent with the protocol for access to HR records and sensitive employment information set out in Part 3.

Health and safety roles and responsibilities

265. Police provides agreed workplace health, safety, and wellbeing systems and specialist support as part of the hosted corporate services model. FSE remains

responsible for identifying and managing risks arising from FSE-directed work, regulatory field activity, and staff performing FSE functions, so far as those matters are within FSE's influence and control. Police remains responsible for risks arising from Police-directed work, Police workplaces, Police systems, Police operational activity, and Police staff. Where duties overlap, the agencies will consult, cooperate, and coordinate, without transferring or excluding any duty under the Health and Safety at Work Act 2015.

Financial systems roles and responsibilities

266. The Public Finance Act 1989 also frames the financial systems approach. The Arms Regulator is treated, with necessary modifications, as if it were a departmental agency and Police were its host department. FSE is not a Crown entity, but the model requires a clear performance and funding line for the FSE Chief Executive while using Police's departmental systems, controls, assets, liabilities, transaction processes, and financial information.

Corporate finance roles and responsibilities

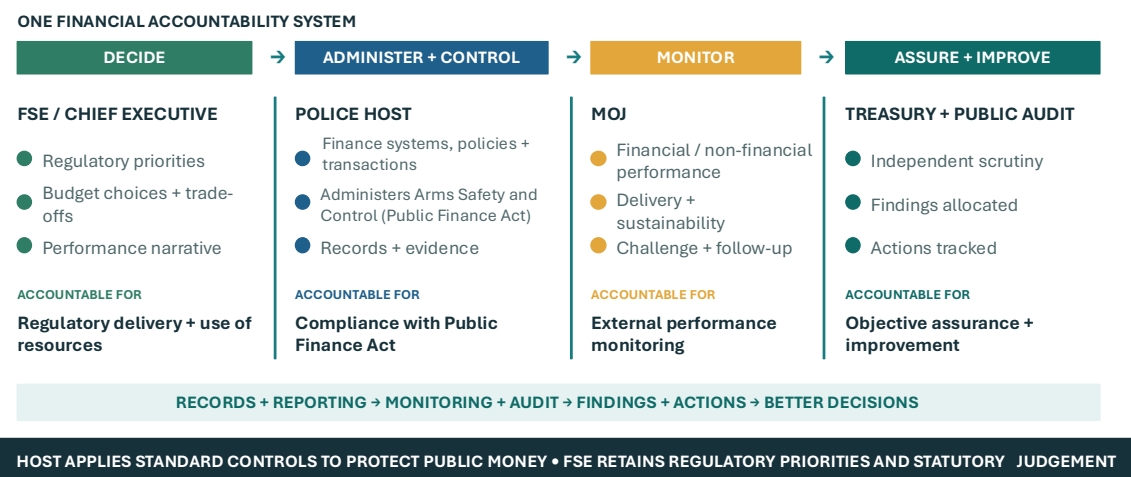
267. Police is responsible for the host-department financial reporting framework, including the preparation, consolidation, and external audit of departmental financial statements that include FSE-related financial information. FSE is responsible for the regulatory decisions, expenditure choices, approvals, assumptions, and performance information that relate to its functions and that are reflected in those statements. Police's financial controls and audit responsibilities enable accurate, and auditable reporting; they do not transfer responsibility for FSE's statutory functions or give Police a policy veto over FSE's regulatory priorities.

268. Where a financial reporting or audit issue arises, the parties will first identify whether the issue concerns accountability for FSE's regulatory activity, control of Police's financial systems and reporting framework, or decision rights over the use of FSE resources. That distinction will determine whether the matter is owned by FSE, owned by Police, or requires joint action.

WORKING ARRANGEMENT | CORPORATE SERVICES

Accountability is shared; decision rights stay distinct

FSE decides; Police administers and controls; MOJ monitors; independent assurance tests the system.



39

Costs for regulatory and corporate services for year one

269. The Year 1 cost-recovery approach for regulatory services is a starting position. For activities that are already subject to cost recovery, and where the level of service expected by FSE is like what has been provided under the current cost recovery agreement, the starting position is continuation of the current contribution plus indexation.
270. Where additional Police groups are now identified as providing cost-recovery services to FSE, or where FSE requires an increase in service levels for existing services, the cost recovery for those additional services should be based on a marginal cost basis.
271. Using a marginal cost basis, FSE would only pay for the incremental cost of resources required to process the specific transaction or provide the additional services. This would still be considered a Year 1 starting point.
- ### First year full review
272. The level of service and the actual and reasonable cost of providing those services will still be subject to a full review during Year 1.

273. A full review in Year 1 will include development of a costing and funding model that is fiscally transparent, proportionate to administer, and capable of being reset or revised as the arrangement develops and circumstances change. The review will identify material cost movements, test the Year 1 assumptions against actual service levels, volumes, and reasonable costs, and complete a true-up process before the end of the 2026/27 financial year. The review may identify opportunities to improve the efficiency, transparency and sustainability of the cost-recovery and funding models. The review may also identify whether any fiscally neutral adjustment to baselines, appropriations, fees-revenue, cost-recovery settings are required. Any proposed changes would be considered and progressed through the appropriate governance, budgetary, and inter-agency approval processes.

Guiding principles to inform the approach to cost modelling

- Both parties acknowledge and agree that the financial arrangements require further analysis
- The further analysis needs to include reviewing the current service offering and which should be cost recovered (including any funding adjustments between Police and FSENZ) or services provided by Police at no cost to FSENZ (from Police baseline)
- The underlying principle is that FSENZ should pay for the services purchased from Police, unless the service is already provided from Police baseline
- Neither party should be disadvantaged through the Year One baseline cost modelling process
- The parties will work to create a more accurate Year One baseline cost model by 31 October 2026

Information sharing for corporate services

274. Corporate services depend on routine information sharing between Police and FSE. That sharing may include employment, finance, ICT, property, procurement, governance, legal, communications, records, audit, assurance, security, privacy, and service-management information. Information may be shared where it is needed to deliver an agreed corporate service, meet an employment or public finance obligation, administer Police-hosted systems, manage access or security, support governance or Ministerial servicing, respond to an audit or assurance process, manage a legal, privacy or OIA matter, or maintain business continuity.
275. Corporate information sharing is limited to the purpose for which the information is shared. It does not create general access to Police information, FSE information, employment records, financial records, legal material, governance

material, communications material, or corporate repositories. Access should be role-based, purpose-limited, proportionate, secure, and auditable where the relevant system allows. Sensitive HR material, legal material, security information, commercially sensitive information, and confidential corporate records should be handled with additional care.

276. This corporate information-sharing setting is separate from operational or regulatory information sharing under the Arms Act. Access to Arms Act operational systems, firearms registry information, licensing information, compliance information, intelligence, vetting material, Police operational information, or law-enforcement information must be authorised through the relevant operational, regulatory, privacy, information-sharing, security, system-access, or delegation arrangement. Corporate service access must not be used as a workaround for operational or regulatory information access.
277. Where information is created, stored, or managed in Police-hosted systems for FSE corporate purposes, the agencies should identify who owns the business record, where it is filed, who may access it, how it will be retained, how it may be searched for OIA, Privacy Act, audit, legal, or assurance purposes, and how unrelated Police or FSE information will be protected. Corporate records should remain discoverable, protected, retained, and managed consistently with privacy, confidentiality, security, public-records, audit, and information-management obligations.

Public records and disposal

278. Information created or held by FSE, including information held in Police-hosted systems on FSE's behalf, will be retained, reviewed, and disposed of in accordance with the Police disposal authority and the Public Records Act 2005. The agencies will apply practical arrangements for record ownership, filing, access, retention, search, and disposal where FSE corporate records are held in Police systems.

ICT roles and responsibilities

279. Police will provide the corporate and operational ICT platforms, identity services, devices, licences, access management, service help desk channels, cyber controls, system administration, and standard support needed for FSE to operate from commencement using Police-hosted infrastructure.
280. Police's corporate ICT role supports continuity, security, records management, access control, and lawful administration. It does not give Police decision rights

over FSE's regulatory priorities, information holdings, public-facing identity, or future technology strategy, except where Police must apply host-system, cyber security, supplier, access, or public-sector ICT controls.

Premises and fleet

281. Police will provide the property, accommodation, facilities, fleet, and related support needed for FSE to operate from commencement, including through Police-hosted sites, shared premises, FSE-specific spaces, and agreed operational locations. These are enabling services. They support continuity and safe delivery but do not give Police control over FSE's regulatory priorities, public-facing service model, regional engagement, or use of funding for statutory functions.
282. The transition-year approach should preserve existing premises and fleet arrangements where needed, while avoiding lock-in of existing settings before demand, footprint, public-facing identity, safety, privacy, secure storage, fleet use, and cost drivers are understood. Police manages the host property and fleet machinery; FSE defines the business need and funding case; and cost treatment should be agreed, evidenced, reviewable, and linked to the service actually provided.

Day-one arrangements preserve continuity

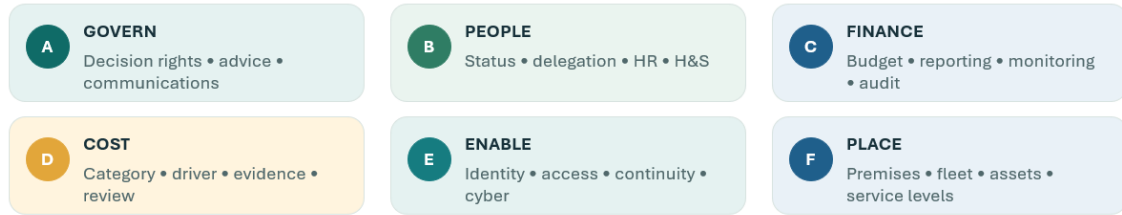
283. The Corporate Services Schedule is a Day 1 continuity tool, not a complete operating manual. It records the key services, owners, request paths, approvals, limits, cost treatment, and known issues sufficiently to support commencement.
284. More detailed requirements may sit in financial delegations, employment instruments, operational guidance, system-access approvals, information-sharing agreements, privacy and security procedures, standard operating procedures, training materials, local practice notes, future schedule updates, or later working arrangements.

WORKING ARRANGEMENT | CORPORATE SERVICES

Corporate readiness requires six controls to work together

Day 1 continuity depends on explicit decisions, usable systems and visible accountability across every appendix.

DAY 1 CONTROL SET



READINESS GATE 1 Authority recorded 2 Access tested 3 Budget visible 4 Risks assigned 5 Service owners named

Evidence of all five controls is required before shared services are treated as operationally ready.

CONTINUITY IS THE OUTCOME • CLEAR BOUNDARIES, CONTROLLED ACCESS AND ACCOUNTABLE DECISIONS ARE THE METHOD

Review of Corporate and Regulatory Services (costs and delivery)

Purpose of review

285. Police and FSE will keep the Corporate Services under active review after commencement. Review is not limited to whether services are being delivered. Regular review also includes the financial and corporate performance of purchased Regulatory Services under Part 2 where those services involve purchasing arrangements, service standards, price, volumes, cost drivers, affordability, cost attribution, funding or fees assumptions, service-provider performance, or unresolved commercial or corporate delivery issues. Operational coordination and collaboration, safety, information-sharing, handover, public-safety, and statutory role-boundary issues remain for review under Part 1.
286. Corporate stewardship means FSE remains accountable for organisational capability, culture, priorities, performance, financial stewardship, and regulatory outcomes. Police remains accountable for the systems, platforms, finance controls, finance policies and processes, and services it has agreed to provide. Accountability must not drift to Police by practice simply because Police controls key infrastructure or records.
287. Urgent, day-to-day, and business-as-usual service issues should be managed through the working-level escalation paths identified in the Corporate Services Schedule and relevant appendices. Quarterly review is not a substitute for those pathways. Its purpose is to identify recurring issues, unresolved decisions, systemic risks, service pressures, and matters that require functional lead, senior agency, Chief Executive, Ministerial, monitoring, audit, privacy, security, or public finance attention.

Quarterly review focus

288. Quarterly corporate stewardship reviews will look across all appendices for systemic escalation points and risks that may not be material in one service line but become material across the hosted model. The scope includes:
- a. **cost allocation and funding-model risk:** whether costs for Arms Act regulatory services, corporate services, ICT dependencies, vendor work, and future change are being attributed to the right funding source, with enough evidence for FSE, Police, Treasury, Ministers, audit, and fee-setting purposes;

- b. **independence and role-confusion risk:** whether Police host controls, systems, language, approvals, employment settings, premises, branding, or service channels are drifting into FSE regulatory decision-making, organisational culture, or public-facing identity;
- c. **service continuity risk:** whether HR, finance, ICT, property, fleet, governance, legal, policy, communications, records, procurement, and other essential corporate services are available, timely, secure, lawful, scalable, and aligned with the relevant schedule;
- d. **health and safety risk:** whether overlapping PCBU duties are being met in practice, including clear consultation, cooperation, coordination, notification, corrective action, and assurance where Regulator staff and Police staff work across shared systems, workplaces, or operational settings;
- e. **information, privacy, records and cyber risk:** whether corporate information sharing, HR records, finance records, legal material, commercial information, OIA and Privacy Act discoverability, public records obligations, audit trails, system access, identity services, and cyber controls are managed without blurring operational Arms Act information holdings or creating inappropriate access;
- f. **commercial, property and physical-security risk:** whether procurement, contract ownership, supplier management, premises, fleet, secure storage, physical security, and facilities support are clear enough to support FSE delivery without turning Police process support into Police approval rights over FSE choices;
- g. **governance, advice and communications risk:** whether advice lines, Ministerial routes, legal privilege, OIA ownership, communications approvals, joint products, records locations, public messaging, and shared stewardship issues remain clear;
- h. **embedded transition-settings risk:** whether temporary workarounds, light-touch controls, and reduced transparency become embedded before service demand, cost drivers, safety impacts, privacy settings, and accountability consequences are understood; and
- i. **systemic escalation risk:** whether repeated issues show that the Schedule, service delivery model, funding model, access settings, escalation paths, policy assumptions, or delegations need to change.

Review outputs

289. Review outputs should be practical and traceable. They may include updates to the Corporate Services Schedule, changes to service delivery models, clarified decision rights, corrected access settings, updated service owners or working-level contacts, revised resourcing and cost assumptions, updated escalation paths, action owners and due dates, expiry of temporary transition settings, matters for the unresolved issues log, and issues requiring Chief Executive,

Commissioner of Police, Ministerial, Ministry of Justice, Treasury, audit, privacy, security, or functional lead attention.

290. Financial issues and culture risks are standing review items. Regular review should test whether the financial model remains fair and transparent; whether Year 1 assumptions are becoming embedded before they are understood; whether Police is recovering only agreed or properly attributable costs; whether FSE has visibility of demand and cost drivers; and whether the degree of reliance on Police systems, people, premises, policies, or service channels remains necessary and proportionate.
291. Reviews should not reopen FSE regulatory decisions or Police operational command decisions. They may review corporate support arrangements where those arrangements affect service continuity, lawful administration, auditability, governance, independence, or either agency's ability to meet statutory responsibilities.
292. Unresolved matters should be escalated where they affect statutory independence, financial sustainability, audit or public finance accountability, service continuity, serious information risk, workforce stability, Ministerial accountability, public confidence, or material constraints on regulatory decision-making.

Escalation pathway

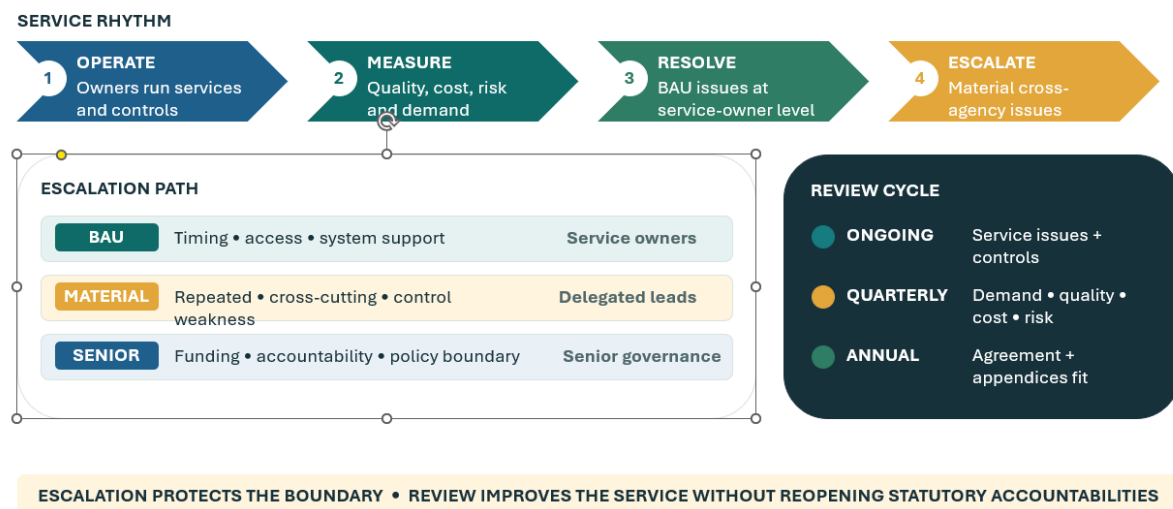
293. Escalation should be tiered. Working-level leads should manage urgent, day-to-day, and business-as-usual service issues. Functional leads should manage unresolved or cross-functional service issues. Quarterly review should identify repeated or systemic issues. Chief Executive and/or Police Commissioner escalation should be reserved for material independence, funding, statutory delivery, service continuity, public confidence, or unresolved inter-agency issues. Ministerial, Ministry of Justice, Treasury, audit, privacy, security, or other specialist escalation should occur only where the matter properly engages those accountabilities.

294. Where escalation is required, the issue should identify the decision needed, the agency or role with authority to decide, the legal, financial, service, information, workforce, or public-confidence implications, the interim operating position, the recommended pathway, and any reporting required to Chief Executives, Commissioners, Ministers, the Ministry of Justice, Treasury, the Auditor-General, privacy or security leads, or other relevant decision-makers.

WORKING ARRANGEMENT | CORPORATE SERVICES

Corporate stewardship keeps the model fit for purpose

Service issues should be resolved close to delivery, with material questions moved to the right authority.



Annual review

295. The annual corporate stewardship review will draw on quarterly evidence and test:

- whether the hosted model still supports FSE's autonomy, culture, financial sustainability, public finance accountability, audit readiness, and statutory delivery;
- which services should continue, change, mature, be repriced, or be considered for exit or replacement;
- whether cost assumptions, service volumes, transition settings, escalation pathways, and relationship roles remain fit for purpose; and
- which issues require Ministerial, Ministry of Justice, Treasury, audit, or senior agency attention.

296. The review process is part of the governance architecture for the autonomous agency model. It supports, but does not replace, statutory accountability, public finance accountability, audit, or Ministerial oversight.

Part 3: Governance, legal, policy and communications

Purpose and service description

297. This section records Police support for FSE's governance, executive support, legal, policy, Ministerial, Privacy Act, Official Information Act, Parliamentary, records, knowledge management, and communications functions. Role clarity is needed because FSE will use Police-hosted systems and processes while exercising separate statutory responsibilities and advising a separate Minister on firearms regulation.
298. Services may include governance and executive support, senior leadership coordination, Ministerial servicing, Cabinet and Parliamentary processes, OIA and Privacy Act support, correspondence, records and knowledge management, legal and policy support, communications and media support, monitoring and reporting, and access to the systems and templates used for those services.
299. The intent is continuity with clear boundaries: Police provides practical support, systems, and process capability; FSE retains its advisory role, decision rights, records ownership, quality assurance, and Ministerial accountability for regulatory functions. The agencies may coordinate on shared Arms Act interests, but they do not advise the same Minister, speak from the same statutory role, or make decisions from the same institutional perspective.

Operating context

300. FSE's Chief Executive is responsible for regulatory functions under the Arms Act and reports to the Minister Responsible for Firearms on those functions. Police remain responsible for policing, law enforcement, public safety, offences under the Arms Act, and report to the Minister of Police on those matters. Both agencies therefore have legitimate interests in the safe operation of the Arms Act system, but those interests are not identical.
301. There is a shared operational stewardship interest in firearms safety, public safety, registry integrity, frontline safety, licence-holder safety, information sharing, public confidence, and the effective operation of the Arms Act. That shared interest means the agencies will need to share information, coordinate operational positions, identify whole-system risks, manage public communications, and sometimes develop joint advice or joint products.

302. At the same time, governance, legal, policy, communications, Ministerials, Privacy Act, Official Information Act, and Parliamentary servicing activities require role clarity. Staff should understand when they are supporting FSE as an autonomous regulator, when they are supporting Police as a policing agency, when advice is being developed jointly, and when information is being shared only for awareness, consistency, risk management, or lawful corporate support.
303. The central distinction is between shared operational stewardship and separate advisory accountability. Shared stewardship supports cooperation on information, safety, operational risk, public confidence, system settings, and implementation issues. Separate advisory accountability protects each agency's ability to provide clear, independent, role-appropriate advice to its own Minister and decision-makers.

WORKING ARRANGEMENT | CORPORATE SERVICES

Shared stewardship, separate accountability

Police provides systems and process support; FSE retains its advice line, decision rights, records and Ministerial accountability.

FOUR SUPPORT LANES

GOVERNANCE	Executive support • Ministerials • Cabinet + Parliamentary processes	Police provides process capability; FSE retains its Chief Executive, governance and Ministerial accountability
ADVICE	Separate • coordinated • joint — agree the mode at the start	Share facts, risks and timing without requiring endorsement of the other agency's judgement
LEGAL + INFO	Legal • OIA • Privacy • records + knowledge management	Name owner, access, filing, retention + disclosure; corporate tools must not bypass operational controls
COMMS	Media • public messaging • joint products	For joint work, agree the lead, approvals, legal review, record location and disagreement pathway

SHARE FACTS + RISKS • KEEP ADVICE LINES, DECISION RIGHTS, RECORDS + MINISTERIAL ACCOUNTABILITY DISTINCT

33

Shared stewardship of advice

304. Police and FSE may develop or share advice and recommendations in three broad contexts:
- separate advice**, where one agency is advising its own Minister, Chief Executive, statutory decision-maker, senior leadership team, or governance forum on matters within that agency's role;
 - coordinated advice**, where each agency retains its own advice line but shares relevant factual and evidence-based material, risk information,

operational context, or proposed timing so that Ministers and decision-makers receive coherent and accurate information; and

- c. **joint advice or joint products**, where the agencies agree that advice, communications, governance material, or implementation products are being developed under a shared operational stewardship arrangement.
305. Separate advice should remain separate until it has been provided to, and returned through, the relevant agency's Ministerial or decision-making process, unless the agency responsible for the advice gives permission for earlier sharing. This protects role clarity, legal confidence, Ministerial accountability, quality assurance, and the integrity of the advice process, whilst maintaining scope for coordinated advice on matters of operational stewardship.
306. Coordinated advice may involve sharing factual and evidence-based information, system data, operational context, timelines, risk issues, implementation dependencies, and agreed background material. It should not require one agency to endorse the other agency's recommendations, policy judgement, legal view, communications position, or Ministerial framing unless that has been agreed.
307. Joint advice or joint products should be identified expressly at the start. The agencies should agree the purpose, lead agency, approving decision-maker, Ministerial route, quality-assurance process, legal review, communications approach, records location, disclosure settings, and how disagreements will be handled before advice or public material is finalised.
308. Where advice relates to coordinated or shared operational stewardship of Arms Act operations, the agencies should be open with each other about safety risks, implementation issues, data quality, frontline impacts, licence-holder impacts, operational dependencies, public confidence issues, and information-sharing requirements. That does not remove the need to keep decision rights and advice lines clear.

Records and knowledge management

309. FSE corporate records may sit in Police-hosted systems, but the agencies should still identify whether a record belongs to FSE, Police, or both agencies for a shared corporate or stewardship purpose.

- 310. For FSE corporate records, the agencies should agree record ownership, filing location, access group, retention approach, and treatment for OIA, Privacy Act, audit, legal, assurance, Ministerial, Parliamentary, and reporting purposes.
- 311. Police may provide corporate repositories, templates, search support, retention tools, and information-management advice. FSE remains responsible for the substance, quality, and use of its corporate records.
- 312. Access to corporate records should be role-based, purpose-limited, secure, and reviewable. Sensitive material should be accessed only where needed for an agreed service, lawful process, audit, assurance, legal obligation, information request, or shared stewardship purpose.
- 313. Corporate records settings should remain separate from operational and regulatory Arms Act information holdings unless a lawful access, sharing, or records-management basis applies. Corporate tools must not be used to avoid operational information-sharing controls, system-access permissions, privacy settings, or delegation requirements.

Part 3: People and culture

Purpose and service description

314. Police will provide human resources and people-related services to support FSE to operate as an autonomous agency within the hosted environment. These services are provided to comply with the Arms Act, preserve business continuity, support staff transition, meet employment obligations, and ensure FSE has access to the core people systems and specialist HR capability it needs from commencement.
315. The services may include payroll administration, employment records management, HR advisory support, employee relations support, recruitment and onboarding support, learning and development administration, health, safety and wellbeing support, workforce reporting, position management, people-related policy advice, and support for organisational change processes where Police policies and processes apply to Regulator staff.
316. Resources required to deliver the HR and employment services articulated in this document and the Corporate Services Schedule will be provided by New Zealand Police.
317. The service is a corporate support service. It does not authorise Police to influence, direct, or determine FSE's regulatory decisions. HR services must support FSE's organisational capability while respecting that Regulator staff are exercising functions within a separate statutory regulatory mandate.

Service boundary framework for people and culture services

318. The Corporate Services Schedule records the agreed HR and people-related service package at a practical level. This appendix explains how those services are bounded by employment status, statutory authority, corporate support responsibilities, and FSE's autonomous regulatory role. It distinguishes what Police provides as host agency, what FSE owns as regulator, and where the agencies must coordinate without merging their respective accountabilities.

Roles and responsibilities – limits and boundaries

319. Police provides the agreed HR systems and employment support needed for FSE to operate in the hosted model, including payroll, employment records, recruitment and onboarding support, learning administration, workforce reporting, and related people processes.

- 320. Police remains responsible for the integrity and administration of Police employment systems, records, payroll processes, HR advice, and employment settings that continue to apply to Regulator staff as Police employees.
- 321. FSE is accountable for the people capability needed to deliver its statutory functions. This includes workforce priorities, role requirements, regulatory capability, training compliance, competency assurance, day-to-day performance expectations, return-to-work outcomes, injury management performance, and oversight of associated people and safety risks.
- 322. Police will support these responsibilities through systems, advice, training platforms, HR processes, injury management support, and reporting, but FSE managers remain accountable for ensuring the requirements are met in the FSE work context.
- 323. The agencies will coordinate where an issue involves both employment settings and FSE regulatory work. Police will advise on employment process; FSE remains responsible for employment matters relating to regulatory judgement and the capability of staff performing FSE functions.
- 324. If the Chief Executive is considering departing from and/or determines that FSEnz will depart from Police processes/policies (as provided for in s 307(7) of the Arms Act), the Chief Executive must develop or alter these and manage any such processes/policies using their Regulator staff or obtain external support (including policy advisors, legal advisors, HR support) and assumes all associated liability.
- 325. The working principle is simple: Police provides the people services for all FSEnz staff with any decisions being made by the appropriate delegation holder; and FSEnz will pay Police for the provision of those services.

Protocol for access to HR records and sensitive employment information

- 326. Police HR staff may access Regulator staff employment information where needed to deliver agreed HR services, meet employer obligations, support the Chief Executive's people-management responsibilities, or maintain Police-hosted HR systems.

- 327. Because FSE and Police employment records may sit in the same Police systems, Day 1 controls should focus on disciplined access rather than eliminating all technical visibility. Access should be role-based, purpose-limited, proportionate, logged where possible, reviewable, and exercised with restraint.
- 328. Police HR staff and Chief Executive support staff should access sensitive people information only where it is needed for an agreed HR, employment, payroll, recruitment, onboarding, offboarding, learning, health and safety, security, audit, workforce reporting, or management process.
- 329. Neither agency should browse, search, or use sensitive staff information without a clear business need and lawful purpose.
- 330. Where a matter needs joint handling, the agencies should agree the purpose of access, who needs to see the records, what material is needed, where it will be filed, and any confidentiality limits before detailed employment material is shared.
- 331. Access discipline should be supported by appropriate access groups, manager approvals, access reviews, confidentiality expectations, privacy training, information-security controls, incident reporting, and audit logs where available.
- 332. The aim is to let Police run the hosted HR service while maintaining confidence that sensitive people information is accessed only for legitimate employment, corporate, workforce, security, audit, or statutory purposes.

Adoption of policies and procedures

- 333. Regulator staff remain Police employees. Police employment agreements, collective agreements, employment policies and processes, payroll arrangements, employment records processes, leave, remuneration, benefits, conduct standards, and other ordinary employment settings continue to apply. Any role for the Chief Executive or FSE managers in hiring, performance management, discipline, dismissal, remuneration, or other employment practices must be supported by the relevant employment agreement, policy, Commissioner delegation, agreed instrument, or other lawful authority.
- 334. Regulator staff are also subject to the New Zealand Police Code of Conduct and related integrity, conduct, information-management, and workplace-behaviour policies that apply to Police employees. New Regulator staff should acknowledge those requirements through the relevant onboarding, employment

agreement, policy acknowledgement, or other lawful process. Those obligations apply as employment and conduct requirements; they do not give Police authority to direct FSE regulatory decisions.

FSE-specific regulatory expectations

335. FSE may set additional role-specific expectations for regulatory conduct, service culture, independence, impartiality, public-facing behaviour, and the proper exercise of delegated Arms Regulator functions. Where Police conduct standards and FSE regulatory expectations both apply, the agencies will identify whether the issue is primarily an employment matter, a conduct or integrity matter, a regulatory accountability matter, an information management or privacy matter, a health, safety, and wellbeing matter, or a mixed matter requiring joint triage and management.

Mandatory induction and compliance training

336. Regulator staff must complete, or have recognised as current, mandatory Police induction and compliance training that applies to Police employees working in the hosted environment. This includes, at a minimum:
- a. Police induction training;
 - b. Police Code of Conduct training and declaration of acceptance;
 - c. integrity and conflicts of interest training;
 - d. privacy and information handling training;
 - e. information security and cyber security training;
 - f. Official Information Act, Privacy Act, and records management training;
 - g. protected disclosures and speaking-up pathways including under the Protected Disclosures (Protection of Whistleblowers) Act 2022;
 - h. workplace health, safety, and wellbeing training;
 - i. bullying, harassment, discrimination, and respectful workplace training;
 - j. use of Police systems, devices, premises, vehicles, and resources;
 - k. security, vetting, access, and identity requirements; and
 - l. any role-specific firearms regulatory, delegation, or public-contact training required by FSE.

Training records and follow-up responsibilities

337. Police are responsible for providing access to the relevant Police policies, systems, training modules, learning records, Code of Conduct attestation processes, and employment-support processes. Police is also responsible for

maintaining employment records that show completion, renewal, or non-compliance with required training.

338. FSE is responsible for addressing non-compliance and for identifying any additional regulatory training, delegation training, public-facing service expectations, independence requirements, cultural capability requirements, health and safety, or operating guidance needed for Regulator staff performing Arms Regulator functions. FSE will also identify where Police induction training needs to be supplemented.

Main risk

339. There is likely to be an increase in demand for services by FSE, above the current baseline, due to the implementation of FSE and associated uncertainty. This may place increased pressure on Police HR employees and resources.

Part 3: Health and safety

Operational safety and workplace health and safety

340. Health and safety requires distinct treatment because firearms regulation places Regulator staff within a risk environment closely connected to frontline Police operations. This Working Arrangement distinguishes operational safety matters, managed through Part 1, from workplace health, safety, and wellbeing matters, managed through Part 3. That distinction is practical and legal, but it does not remove the overlap between the two. The same event may require a Police operational response, IPCA consideration, or public-safety escalation under Part 1, while also requiring workplace health and safety reporting, staff support, corrective action, assurance, or WorkSafe assessment under Part 3.

Overlapping HSWA duties

341. Under the Health and Safety at Work Act 2015, duties may sit with more than one duty holder and may overlap. This Working Arrangement cannot transfer or exclude those duties. It allocates practical responsibilities for systems, support, coordination, notification, assurance, escalation, and review, having regard to each agency's work, workers, workplaces, and degree of influence and control. FSE will use Police health and safety systems, reporting channels and specialist support where that is necessary for continuity, shared risk visibility, and timely operational assistance. That shared infrastructure does not transfer accountability: the Chief Executive remains responsible for managing risks arising from FSE work, while Police remains responsible for policing responses, Police workplaces, Police systems, and risks within Police operations.

Accountability within influence and control

342. The accountability principle is that everyone involved in the work has health and safety responsibilities, and the Commissioner, the Chief Executive, officers, and senior leaders must each meet the duties that apply within their role and sphere of influence and control. Police and FSE may agree who will provide systems, advice, reporting channels, wellness support, and practical coordination, but those arrangements do not displace the statutory duties that apply to each duty holder under the Health and Safety at Work Act 2015.

Relationship with Part 1 and IPCA pathways

343. This section should be read with Part 1. Public and personal safety, Police operational response, critical-incident management, and IPCA-related pathways are managed through the Operations Header where regulatory and policing functions meet. The Arms Act also brings Arms Regulator functions

within IPCA oversight in relevant circumstances. That reinforces that FSE remains accountable for the regulatory decisions, delegations, records, and conduct of Arms Regulator functions that may sit alongside, or contribute to, a wider health and safety or operational-safety event.

Health, Safety and Wellbeing Schedule

344. The Health, Safety and Wellbeing Schedule will give practical effect to this section. It will cover the agreed approach to health and safety systems, wellness services, return-to-work support, ACC and Accredited Employer Programme processes, critical-risk programmes, governance, reporting, assurance, specialist adviser support, training, relationship-manager roles, incident notification, and escalation for mixed operational and workplace safety matters. The schedule is intended to support consultation, cooperation, and coordination between the agencies, not to reallocate statutory duties.

Senior governance and shared risk visibility

345. To support senior visibility of overlapping duties and shared risk, the Chief Executive will be invited to participate in the Commissioner's Health and Safety Governance Group (HSGG), or any successor senior health and safety governance forum, where matters affecting Regulator staff, Police staff, shared work, shared workplaces, or mixed operational and workplace safety risks are considered.

WORKING ARRANGEMENT | CORPORATE SERVICES

One event can engage two safety pathways

Operational response and workplace health and safety run in parallel; shared systems coordinate action without reallocating statutory duties.



38

Boundary constraints and limits

- 346. Police HR support and employment settings enable the hosted model; they do not give Police influence over FSE regulatory decisions, regulatory priorities, or the exercise of Arms Regulator functions.
- 347. People issues should be triaged by their substance: employment, conduct, security, regulatory accountability, Police operational matter, health and safety, or a mixed issue requiring coordinated handling.
- 348. FSE leads where the issue affects regulatory capability, independence, public confidence, or continuity of regulatory service. Police may support process or employment decisions only where the relevant employment, security, delegation, or statutory authority applies.
- 349. Health and safety matters must use the agreed H&S pathways and, where public safety, Police response, or IPCA issues are also engaged, be coordinated with Part 1.

Main delivery risks

- uncertainty about employment and/or health and safety permissions and obligations may continue – for example, when Constables are acting under delegation for Regulatory Services;
- overlapping health and safety and PCBU duties may be unclear in practice, creating gaps in consultation, cooperation, coordination, notification, corrective action, or assurance where Regulator staff work in Police-hosted workplaces or alongside Police operational activity; and
- mixed incidents may be handled through only one pathway, rather than being triaged for both Part 1 operational safety/public-safety requirements and Part 3 workplace health, safety, wellbeing, reporting, and assurance requirements.

Transitional issues and interim review

- 350. For Day 1, FSE needs stable people, employment, and health and safety services. Police and FSE should confirm the essential service map, relationship leads, role-boundary guidance, health and safety access, and mixed-issue escalation routes.

351. Early review should test whether the Day 1 settings remain workable, need fuller guidance or training, or require escalation because of recurring HR issues, health and safety issues, mixed operational/workplace safety matters, or unclear role boundaries.

Part 3: Finance and annual budget services

Purpose and service description

352. Police is the administering department for FSE under the Public Finance Act 1989. Police administers the Arms Safety and Control output class, and supports FSE's access to financial systems and policies within the hosted environment. The purpose of the service is to ensure FSE can operate as an autonomous agency while continuing to use Police financial infrastructure and support where required for continuity.
353. The services may include payment processing, accounts payable and receivable, purchase order support, external financial reporting, cost centre administration, financial delegations support, appropriation and funding advice.
354. Finance services must make costs visible and reviewable. The service should distinguish between baseline Police corporate overheads, incremental costs caused by the autonomous FSE model, transition costs, and activity-driven services that may require separate approval or charging.

Autonomous-agency financial framework

355. The Public Finance Act 1989 applies to the Arms Regulator, with necessary modifications, as if the Arms Regulator were a departmental agency and New Zealand Police were its host department. That creates a bespoke autonomous-agency model. FSE is not a Crown entity, but the model preserves a separate performance and accountability line for the Chief Executive while using Police's departmental systems and controls.

Appropriation structure and Ministerial accountability

356. In plain terms, the firearms regulatory appropriation sits within Vote Police, and Police administers that appropriation. However, the funding arrangements need to protect the independence of the Arms Regulator. This means the Minister Responsible for Firearms is treated as the Appropriation Minister for that funding, and the Chief Executive is responsible for managing the appropriation for firearms regulatory purposes.

357. For the purpose of administering the Arms Safety and Control output class, Police will work closely with FSE so FSE is consulted on appropriation risks and opportunities, and the Minister Responsible for Firearms is advised in the Minister's capacity as Appropriation Minister.

Finance controls and regulatory independence

358. The core boundary is that Police finance controls support lawful administration; they do not give Police general decision-making rights over the Chief Executive's regulatory priorities, allocation of FSE funding, performance intentions, or advice to the Minister Responsible for Firearms. Police will provide access to host finance, systems, accounting processes, delegations support, transaction processing, audit trails, and financial information that sit within Police infrastructure.
359. FSE remains responsible for the regulatory purpose, funding strategy, prioritisation, demand signal, performance story, and explanation of what is delivered with the funding provided for the regulator. The Chief Executive may operate outside Police's strategic and policy framework but may not manage assets and liabilities. Police therefore retains proper host-department control over assets, liabilities, systems, and corporate financial controls, while FSE retains decision rights over how its funding is applied to deliver its statutory regulatory functions.

Budget, Estimates and performance information

360. In the public finance cycle, FSE should lead the substantive case for Budget bids, Estimates material, performance information, and advice on regulatory pressures and priorities. Police should support those processes by providing appropriation advice and guidance. Treasury applies the usual central public finance scrutiny. The Ministry of Justice monitors FSE's financial and non-financial performance and supports advice to the Minister Responsible for Firearms.

Audit and evidence

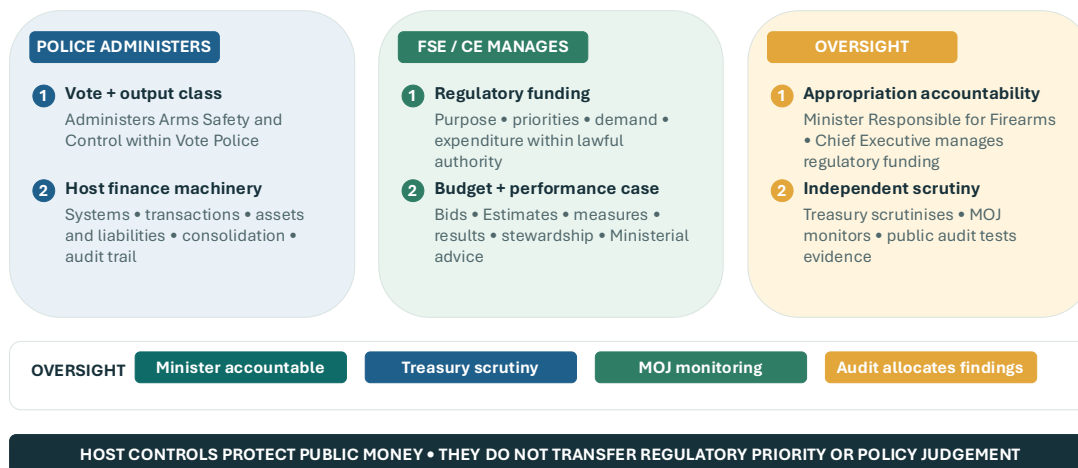
361. The Public Audit Act 2001 also applies to the Arms Regulator. Audit should therefore treat FSE as accountable in its own right for the regulator's performance, stewardship, use of funding, and performance information, in a way analogous to a Crown entity audit. Police is responsible for making its systems, controls, records, audit trails, and evidence available where they support FSE activity, while protecting Police information that is unrelated to the

audit. Audit findings should distinguish between matters FSE owns, matters Police owns as host department, and matters that require joint action.

WORKING ARRANGEMENT | CORPORATE SERVICES

A bespoke public-finance model keeps roles distinct

Police administers Vote machinery; FSE manages regulatory funding and performance within a separate accountability line.



39

Roles and responsibilities

362. FSE is responsible for the regulatory purpose, funding strategy, prioritisation, demand signal, expenditure decisions, performance measures and results, advice to Ministers on regulatory funding pressures, and stewardship of the functions entrusted to it, within approved appropriations, delegations, procurement requirements, and other applicable controls. Police is responsible for providing the agreed finance services, host systems, transaction processes, financial policies and external reporting support to FSE.

Police host-department finance role

363. Police owns and operates the financial processes and policies and external reporting framework which FSE will have access to. FSE will be responsible for its own reporting. This ownership is a Public Finance Act responsibility. It does not transfer responsibility for FSE's statutory functions, regulatory judgements, funding priorities, performance measures, or performance outcomes to Police.

Decision rights and control points

364. The parties will distinguish between the regulatory or prioritisation decision and the accounting, control, or compliance decision. FSE decides what regulatory activities, initiatives, and priorities are funded within its approved authority.

Police decides how those decisions are processed within Police's departmental accounts and compliance with the Public Finance Act.

365. In practical terms, Police answers questions about whether the host financial system can process a transaction within the requirements of the Public Finance Act and as vote administrator. FSE answers questions about which regulatory activities are most important, which expenditure is required, whether a business case or Budget initiative should proceed, whether resources should be reallocated, and how statutory functions should be delivered.
366. Police may decline to process a transaction where it contravenes the requirements of the Public Finance Act. That is a control veto. It must not be used to override FSE's regulatory priorities, substitute Police's policy judgement for FSE's statutory judgement, or prevent FSE from using approved funding for lawful regulatory purposes.

Year-end reporting and audit

367. For year-end reporting and audit, Police is responsible for preparing and supporting the audit of the consolidated departmental financial statements that include FSE-related financial information. FSE will provide timely information, explanations, approvals, assumptions, performance information, and supporting material for FSE-related transactions, commitments, assets, liabilities, cost allocations, accounting judgements, performance measures, and stewardship matters required for Police's financial reporting and audit obligations.

Monitoring role

368. The Ministry of Justice is responsible for monitoring FSE's financial and non-financial performance in respect of the Chief Executive. This monitoring role is distinct from Police's service-provider role. Service information from Police should feed into Ministry monitoring, but Police does not monitor or direct the Chief Executive's performance on behalf of the Minister Responsible for Firearms.

Keeping the finance boundary visible

369. Both agencies are responsible for understanding the limits and permissions of the autonomous agency model. Financial reporting, audit evidence, cost information, and service performance data should support accountability without turning Police's host-department controls into approval rights over FSE's regulatory resource allocation. Where a financial reporting or audit issue arises, the parties should first identify whether it concerns FSE accountability for regulatory decisions, funding choices, performance information, results, and stewardship; Police control of host systems, controls, records, consolidation,

audit trails, and audit evidence; or a shared process requiring joint management action.

Finance services summary

370. The Corporate Services Schedule records the agreed finance service package at a practical level. This section provides the boundary framework for those services, including what Police provides through host-department finance systems and controls, what FSE owns as the autonomous regulator, and where approvals, records, cost treatment, audit evidence, or public finance accountabilities need to remain clear.

WORKING ARRANGEMENT | CORPORATE SERVICES

Corporate finance separates the decision from the process

FSE decides the regulatory purpose and need; Police provides the finance, procurement, reporting and control machinery.

SERVICE CYCLE	POLICE PROVIDES	FSE LEADS / DECIDES	BOUNDARY • EVIDENCE • COST
PLAN + FUND Budget • Estimates • appropriation	Host coding, forecasts, appropriation guidance and external-reporting support	Substantive bids, demand, priorities, measures, performance story and Ministerial advice	Minister is Appropriation Minister; Chief Executive manages regulatory funding
PROCESS + PAY AP • AR • PO • cost centres	Payments, receipting, purchase orders, supplier processes, accounting and audit trails	Lawful business need, regulatory purpose, expenditure choice and approvals within authority	Controls test legality and compliance; a transaction veto is not policy direction
PROCURE + CONTRACT Commercial support	Procurement channels, probity, supplier checks, financial controls and contract records	Need, requirements, approach, evaluation input, relationship and regulatory outcome	Agree the route early for material financial, legal, independence or public-confidence risk
REPORT + AUDIT Monthly • year-end • assurance	Consolidated statements, records, controls, audit evidence and external-reporting support	Explanations, assumptions, performance information, stewardship evidence and remediation	Allocate issues to FSE, Police or joint action; protect unrelated Police information
COST + REVIEW Classify • monitor • improve	Baseline data, cost drivers, allocations, service information and finance advice	Challenge allocations, explain regulatory consequences and assess service value	Separate baseline, autonomous-model, transition and activity-driven costs; MOJ monitors
FSE DECIDES PURPOSE AND PRIORITY • POLICE PROCESSES • CONTROLS PROTECT COMPLIANCE, NOT POLICY DIRECTION			

40

Procurement, commercial and contract support

371. Police will provide procurement, commercial and contract support where FSE needs to buy goods or services using Police-hosted systems, procurement channels, financial controls, supplier processes, or contract administration support. This support enables FSE to operate within lawful public-sector procurement practice while using Police corporate machinery.
372. FSE is responsible for the substantive procurement decision. This includes identifying the business need, confirming the regulatory purpose, setting

requirements, approving the preferred approach within delegations, managing the service relationship, and remaining accountable to the Chief Executive and Minister for procurement choices that support FSE functions.

373. The expected operating position is that FSE follows applicable Police procurement processes and broader public-sector procurement principles, including probity, value for money, fairness, transparency, conflict management, and appropriate recordkeeping. Police may only require process steps that are needed to protect legality, probity, supplier integrity, auditability, contract records, financial controls, and public money.
374. Police procurement support does not give Police general authority to determine whether FSE should procure a service, what regulatory outcome FSE should prioritise, or which lawful option best supports FSE's statutory functions. Where a procurement has material financial, legal, policy, commercial, operational, independence, or public-confidence implications, the agencies should agree the decision route and escalation before commitments are made.

Part 3: Costs for regulatory services and corporate services

Purpose

375. This section sets out the proposed funding approach for the corporate and regulatory services that Police will provide to FSE under the Working Arrangement. Its purpose is to support;

- An interim year one starting point, including a continuation of the current contribution plus indexation
- A full review of true costs during year one.

Allocation of costs under the Working Arrangement

376. Section 315(1) provides that the Commissioner must provide the corporate services and support necessary to enable the Arms Regulator to perform or exercise its functions, duties, and powers, except to the extent that any variation is agreed between the Commissioner and the Chief Executive.

377. Section 315(2) requires the Commissioner and the Chief Executive to agree working arrangements between the Arms Regulator and Police, and to cooperate and collaborate with each other for the purposes of those working arrangements.

378. Section 315(3) requires the working arrangements to set out the resources and administrative support that the Commissioner will provide to the Arms Regulator, and the estimated cost of that support. This means the costing work is not optional. It is part of the legal architecture for making the hosted autonomous agency model transparent, reviewable, and accountable.

Public finance principles for costs and resources

- **Accountability follows funding:** costs should sit where statutory, Ministerial, performance, and audit accountability sits. Costs that support FSE's regulatory functions should be visible to FSE, to Police where Police is providing the service, to Ministers, and to the public finance system.
- **Costs should be attributable, evidenced, and transparent:** Police may recover costs that are properly linked to agreed services, visible cost drivers, reasonable service volumes, or specific transition, corporate, ICT, vendor, assurance, or regulatory-support requirements. Known costs should be transparent from commencement, while recognising that not all service

requirements, cost movements, or cross-agency cost impacts will be fully understood on Day 1.

- **Funding-model choices are policy choices:** decisions that materially shift costs between Crown funding, fees, levies, cost recovery, third-party revenue, Police baseline funding, or FSE's appropriation are not finance administration alone. They must be developed jointly by the agencies, supported by evidence from the review and true-up process, and routed through the appropriate Budget, Treasury, monitoring, and Ministerial processes.
- **Host controls do not displace regulatory accountability:** Police finance systems, controls, delegations, and Vote administration support lawful financial management. They do not substitute for FSE's responsibility for regulatory priorities, service impacts, performance information, or funding needs. Equally, FSE's funding and service expectations should be clear enough for Police to understand the services it is being asked to provide, the costs it may properly recover, and any material cost movements that need to be assessed.
- **Transition settings should not become the funding model by default:** Day 1 arrangements may be pragmatic, but they should be reviewed at six months, 12 months, and before the end of the financial year as demand, service volumes, cost drivers, known costs, cost movements, service levels, safety impacts, privacy settings, and accountability implications become clearer. The review should include a true-up process to provide a shared understanding of actual and reasonable costs, the extent of any cross-subsidy or underfunding, and whether any consequential funding, baseline, appropriation, cost-recovery, or inter-agency adjustment should be considered through the appropriate approval process.

Key risks

- **Fiscal sustainability risk:** the Year 1 starting position may not remain affordable, transparent, or sustainable for either agency if actual service demand, cost drivers, cost movements, or service levels differ materially from the assumptions used at commencement.
- **Cost attribution drift:** costs may be charged to FSE or retained by Police without a clear link to the agreed service, cost driver, service volume, statutory function, or accountability setting, making it harder to assess whether costs are properly attributable and reasonable.
- **Hidden host costs:** ICT, vendor, assurance, corporate overhead, transition, or regulatory-support costs may remain embedded in Police systems or baselines and not be visible enough for Budget, audit, monitoring, fee-setting, cost-recovery, or true-up purposes.

- **Short-term workarounds harden:** Day 1 arrangements may become the default funding or service model before service demand, cost drivers, safety impacts, privacy settings, accountability consequences, and any cross-agency funding impacts are properly understood.
- **Review scope is too narrow:** the Year 1 review may focus on service delivery only, rather than also testing actual and reasonable costs, known cost movements, service levels, volumes, cross-subsidy, affordability, and whether any consequential funding, baseline, appropriation, cost-recovery, or inter-agency adjustment should be considered through the appropriate approval process.

The transitional arrangement for agreed costs for 2026/27 FY

379. Police and FSE have agreed that, for Year 1, the starting position for activities already subject to cost recovery is continuation of the current cost contribution plus indexation, where the level of service expected by FSE is like what has been provided under the current cost recovery agreement.
380. Where additional Police groups are now identified as providing cost recovery services to FSE and/or an increase in service levels for existing services, then the cost recovery for the additional services should be based on a marginal cost basis.
381. On a marginal cost basis, FSE would pay only for the incremental cost of the additional resources required to process the specific transaction or provide the additional service. Evidenced add-ons will identify the service, cost driver, basis of estimate, funding treatment, approval pathway and review or expiry point. Add-ons should be used only where Police can show a clear incremental cost or transition requirement.
382. This Year 1 approach is a starting position only. The level of service, service volumes, cost drivers, and the actual and reasonable cost of providing those services will be subject to review during Year 1.

Improved costing and financial modelling in time for 2027/28

383. The agencies will develop costing and funding models during Year 1 to distinguish what Police must provide as host department, what FSE is accountable for as an autonomous regulator, what is transitional, what is activity-driven, and what is properly attributable to each agency's statutory, service, funding, and accountability responsibilities.

384. A fuller funding assessment of regulatory and corporate service costs will be completed during Year 1, once actual demand, service volumes, cost drivers, known costs, and material cost movements can be more reliably assessed. The FY 2026/27 review will apply the principles set out above and will distinguish baseline Police capability from incremental FSE, transition, activity-driven, and specialist costs. It will provide an evidence-based foundation for the enduring funding and charging model.
385. The review will include a true-up process between the agencies. The true-up process will test the Year 1 assumptions against actual service levels, service volumes, cost drivers, known costs, reasonable costs, and any material cost movements. It will also help identify whether there is any cross-subsidy, under-recovery, over-recovery, or funding pressure that should be addressed through the appropriate approval process.
386. The funding model should align with the public finance cycle. Where the review shows that ongoing costs, resources, or services sit with one agency but accountability sits with the other, the agencies should jointly assess whether any fiscally neutral adjustment to baselines, appropriations, cost-recovery settings, or inter-agency funding arrangements should be considered through the Budget, Treasury, monitoring, Ministerial, or other appropriate approval process.
387. Any such assessment should distinguish existing Police baseline capability, incremental costs of supporting the autonomous regulator, services that should remain Police responsibilities, costs that should sit with FSE, and costs that are transitional only. It should also identify any impacts on Police appropriations and FSE funding. The purpose is to align funding, service expectations, and accountability with the practical cost of delivering the working arrangements, without pre-determining the outcome of the review.
388. Other agencies will be involved where the funding model requires external testing or approval. The Ministry of Justice, as monitoring agency, should test whether the model supports FSE's financial and non-financial performance obligations. Treasury should be involved through the usual fiscal management processes. Police and FSE should provide the cost evidence, assumptions, service scope, known cost movements, and risk analysis needed to support that assessment.

Part 3: Corporate processes, ICT platforms and identity services

Purpose and service description

389. Police will provide ICT platforms, infrastructure, access, devices, support services, cyber controls, and corporate technology services to enable FSE to operate as an autonomous agency within the hosted environment. The purpose of this section is to identify the ICT services Police will supply to FSE as corporate support services, separate from the information systems and operational technology needed to administer and operate the Arms Act.
390. Police ICT services under this section support FSE as an organisation. They include the enterprise platforms, access permissions, service desk channels, devices, network services, cyber security settings, and corporate applications needed for FSE staff to work, communicate, be onboarded, access employment and finance systems, complete mandatory training, use records and knowledge systems, and operate within Police-hosted premises and networks.
391. The services described in this section are provided because FSE will rely on Police-hosted infrastructure and enterprise services at commencement. ICT is a material cost area. The service scope, cost drivers, funding treatment, demand assumptions, service standards, and review points must therefore be visible, evidenced, and capable of being reset as FSE's autonomous operating model matures.
392. This section is limited to corporate ICT platforms and services. It does not set out the full operating model for the Arms Information System, firearms registry systems, firearms-specific telephony, data exchanges, regulatory information holdings, Police operational information systems, or other platforms used to administer the Arms Act.

Service scope

393. Police will provide FSE staff with access to the standard Police enterprise technology environment needed to perform their roles, subject to approved access, identity, security, privacy, and information-management requirements.
394. The corporate identity, security and ICT services may include:

- a. network connectivity and access to Police-hosted ICT infrastructure at agreed Police and FSE sites;
- b. appropriately branded identity and access management, including QID, log-in credentials, Active Directory groups, email accounts, device policies, multi-factor authentication, single sign-on, VPN access where approved,
- c. protective security systems and processes, adjusted to reflect Chief Executive accountability for Regulator staff, along with related access administration to secure facilities;
- d. Police-issued user devices and standard end-user computing services, including laptops, mobility devices, peripherals, standard software, device configuration, technical support, maintenance, refresh, sanitisation, and disposal;
- e. Microsoft 365 and related productivity tools, including email, calendar, Teams, SharePoint, document collaboration, and standard office productivity applications, subject to any agreed constraints on external collaboration, branding, records, information classification, and identity presentation;
- f. ServiceNow or equivalent ICT service management channels for onboarding, access requests, incidents, service requests, hardware requests, workflow initiation, and service reporting;
- g. access to MyPolice or equivalent HRMIS functionality for employment, payroll, leave, remuneration, performance, employee records, and other people-related corporate processes where those systems continue to apply to FSE staff;
- h. access to Police finance systems and related financial administration tools needed for budgeting, procurement, purchase orders, invoices, approvals, financial reporting, cost centre administration, and other host-department finance processes;
- i. access to Police intranet material, Police Instructions, corporate policies, guidance, staff notices, and internal knowledge resources where those materials apply to FSE staff because they remain within Police employment, systems, premises, or security settings;
- j. access to Police online learning platforms and mandatory training modules, including induction, Code of Conduct, privacy, information security, cyber security, records management, health and safety, integrity, conflicts of interest, and other corporate training required for staff working in the hosted environment;
- k. access to SharePoint, filing, document management, knowledge management, public records management tools or processes, and other corporate information repositories used for FSE corporate administration, subject to agreed access controls, records rules, retention and disposal requirements, ownership settings, naming conventions, searchability, auditability, information-management standards, and separation from operational Arms Act information holdings;

- l. help and service desk support, including access request support, incident logging, troubleshooting, hardware and software support, password or account assistance, service-status updates, onboarding and offboarding support, and guidance on where to seek help for Police applications, Police-issued devices, Police-managed products, Police enterprise systems, and access issues;
 - m. patching, monitoring, audit, vulnerability management, security configuration, and lifecycle management for Police ICT-managed servers, devices, accounts, and enterprise services used by FSE;
 - n. cyber security advice, monitoring, incident processes, and protective security controls for Police-managed systems, devices, accounts, networks, and infrastructure used by FSE;
 - o. business-as-usual ICT change management for Police-managed services, including communication of changes that may affect FSE access, availability, integration, records management, privacy, or service continuity; and
 - p. equipment recovery, sanitisation, disposal, and offboarding processes for staff leaving FSE or changing role.
395. Police will provide these services broadly in line with the support provided to Police staff, except where a different service level, priority, process, cost treatment, access setting, or FSE-specific accountability or requirement is agreed.
396. The service scope should identify which services are standard enterprise services, which are FSE-specific incremental services, which are transitional establishment services, which require additional capacity, and which may be varied, repriced, disaggregated, or purchased differently over time.

WORKING ARRANGEMENT | CORPORATE SERVICES

Shared platforms enable FSE

Police supplies corporate ICT; FSE defines identity and need; Arms Act operational systems remain governed separately.



45

Authorising environment

397. The Commissioner will provide the corporate services and support necessary to enable the Arms Regulator to perform or exercise its functions, duties, and powers, except to the extent that the Commissioner and Chief Executive agree a variation. ICT platforms and services are part of that corporate support where they are necessary for FSE to operate as an agency in the hosted environment.
398. ICT access is not regulatory authority. Access to Police enterprise systems, devices, networks, intranet material, HR systems, finance systems, SharePoint, or learning systems supports lawful administration. It does not authorise Police to make FSE regulatory decisions, and it does not authorise FSE staff to access Police operational information unless a separate lawful access basis applies.
399. Each ICT service must have a clear access basis. The basis may include employment status, manager approval, system-owner approval, information-owner approval, a financial delegation, a procurement process, a security approval, a privacy or information-sharing pathway, or another lawful permission. Access should be role-based, purpose-limited, secure, logged where appropriate, and reviewed.
400. Where Police policies, standards, security requirements, acceptable-use rules, information-management rules, or cyber controls apply because FSE is hosted in Police systems, this should be explicit. Where FSE requires different settings to protect its statutory independence, public-facing identity, regulatory

information, or organisational culture, the issue should be recorded and escalated through the agreed governance process.

Branding, identity and protective security

401. FSE also needs its own organisational identity and identification settings, including how staff present as FSE staff, how FSE is distinguished from Police in corporate systems, premises, public-facing settings, email, collaboration tools, identification cards, access credentials, and protective security processes. Police will provide the systems and processes for identity management, identification, premises access, and security controls because those services sit within Police-hosted infrastructure. FSE remains responsible for defining the identity it needs as an autonomous regulator, and both agencies must ensure the hosted processes support that identity without confusing FSE staff with ordinary Police operational staff or creating unintended Police control over FSE's regulatory functions.

Roles and responsibilities

402. Police is responsible for the Police-managed ICT platforms and services used by FSE, including networks, devices, accounts, enterprise applications, Microsoft 365 settings, SharePoint administration, service desk channels, cyber security, patching, monitoring, lifecycle management, and standard ICT support.
403. Police may condition, defer, decline, or escalate ICT requests where needed to protect system integrity, cyber security, privacy, information management, operational resilience, supplier obligations, or lawful administration.
404. FSE is responsible for identifying its business requirements, access needs, regulatory-independence requirements, service-continuity needs, information-management requirements, and FSE-specific ICT demand that may affect cost, capacity, security, or prioritisation. FSE managers are responsible for requesting and confirming role-based access, supporting onboarding and offboarding, ensuring mandatory training is completed, and identifying where Police-hosted systems affect FSE's autonomy, service model, public identity, or regulatory information.
405. Both agencies will keep the service boundary visible. Police provides ICT as host and service provider. FSE remains accountable for its organisational choices, statutory outputs, regulatory information requirements, and business priorities.

Boundary constraints and limits

- Corporate ICT support does not make Police responsible for FSE's regulatory judgements, business decisions, content decisions, statutory advice, or prioritisation of regulatory work.
- Corporate ICT access does not create access to Police operational systems or information. Access to operational, intelligence, registry, licensing, vetting, or firearms-specific systems must use the relevant regulatory, operational, information-sharing, privacy, security, or delegation pathway.
- FSE use of Police intranet material, corporate guidance, policies, and training supports the hosted corporate environment. It does not import Police operational command, law-enforcement priorities, or Police regulatory judgement into FSE's functions.
- Collaboration tools, email, SharePoint, and document repositories should be used in ways that preserve identity, records, privacy, information classification, external collaboration settings, and separation between corporate information and Arms Act operational information.
- Where FSE requires ICT support beyond the standard hosted service, the scope, cost, approval, timing, and service expectations should be agreed before work proceeds.
- Police is not responsible for FSE-procured systems or services unless Police has expressly agreed to provide hosting, integration, security assurance, support, or another defined service.

Cost, demand and service standards

406. ICT costs should be transparent and linked to agreed services, distinguishing standard host services from FSE-specific, transition, capacity, licence, hardware, assurance, site-specific, or project-based costs.
407. Material changes in FSE staff numbers, locations, access needs, collaboration requirements, devices, licences, or system dependencies should be treated as demand changes with cost and capacity implications.
408. Police ICT support will ordinarily be broadly consistent with support available to Police staff, unless another service standard is agreed. Where incidents or dependencies affect FSE service continuity, Police should provide reasonable updates and escalation routes.

409. Changes to Police-managed ICT services that may materially affect FSE access, security, service availability, privacy, records, identity, finance, HR, onboarding, or continuity should be communicated in advance where practicable.

Main delivery risks

410. The main delivery risks are Day 1 access readiness, cost visibility, role and identity clarity, separation between corporate and operational access, records management, access lifecycle controls, external collaboration limits, and service-continuity impacts from Police-wide ICT constraints.

Transitional issues and interim solution options

- The Day 1 priority is stable access to Police-hosted corporate ICT services while FSE's longer-term operating model, identity, records environment, funding model, and technology strategy mature.
- The starting position is continuity of existing Police-hosted corporate ICT services, including standard systems, devices, accounts, licences, service channels, identity management, security settings, and support arrangements.
- The agencies should confirm a practical Day 1 ICT service map covering systems, platforms, accounts, access roles, devices, licences, support channels, records locations, relationship leads, and escalation routes.
- Quarterly review should test whether access, records management, service levels, costs, collaboration settings, identity settings, and cyber controls remain fit for purpose, and whether any Police-hosted corporate services should be varied, repriced, disaggregated, or matured over time.
- ICT systems and information flows used for Arms Act operational and regulatory functions are addressed separately in the Operations Header.

Part 3: Premises, property and fleet

Purpose and service description

411. Police will provide property, accommodation, facilities, fleet, and related support so FSE can operate safely and effectively from Police-hosted sites, FSE-specific sites, shared premises, and agreed operational locations. These are enabling services. They support FSE's statutory functions but do not determine FSE's regulatory priorities, judgements, public-facing service model, or regional operating choices.
412. This section is concerned with practical use and support rather than ownership. It covers access to premises, accommodation planning, desk allocation, public-facing spaces, facilities management, utilities, maintenance, physical security, secure storage, signage, fit-out, moves and changes, fleet leasing, pool-vehicle access, booking tools, fuel cards, insurance, servicing, registration, telematics, user support, and related supplier or contract administration.
413. The transition-year focus is continuity, cost visibility, risk management, and review. Existing property and fleet settings may continue where needed for Day 1, but should be tested as FSE's operating model, footprint, workforce, public-facing service needs, and regional demand become clearer

Legal and public finance framework

414. The Arms Act and Public Finance Act create a host-department control boundary. The Chief Executive has the powers needed to perform Arms Regulator functions but may not manage assets and liabilities. Police therefore retains responsibility for the machinery of property, accommodation, fleet, leases, suppliers, asset systems, financial controls, procurement channels, liabilities, insurance, and related balance-sheet consequences where those sit within Police systems or accounts.
415. FSE remains responsible for defining the statutory, operational, workforce, public-facing, privacy, security, regional, secure-storage, and service-delivery needs that drive its property and fleet demand. FSE also remains responsible for explaining the funding needed for those functions, the service consequences if support is unavailable, and whether the arrangements support its autonomous regulatory identity.

416. The working principle is simple: Police manages the host property and fleet machinery; FSE defines the business need and funding case; and the cost treatment must be agreed, evidenced, reviewable, and linked to the service actually provided.

Current funding position for premises and fleet

417. The current FSA model provides a practical starting point, not an enduring price. It includes baseline property funding, direct pass-through treatment for some attributable property costs, and separate treatment for fleet lease and running costs through Police finance processes.
418. That means the existing position is already mixed: some costs are baseline, some are direct or variable, some are passed through, and some sit outside the fixed corporate operations contribution. The transition year should preserve continuity while making the cost base clearer.

Future-state funding intent

419. The future model should align property and fleet funding with the new statutory accountability model without creating excessive transaction cost. Costs should be transparent, proportionate, and reviewable.
420. The agencies should distinguish between:
- existing Police baseline capability;
 - direct FSE property costs;
 - incremental costs caused by hosting FSE as an autonomous agency;
 - FSE-specific fleet lease and running costs;
 - usage-based costs where charging is practical;
 - transition costs; and
 - broad Police overheads or operational costs that are not properly attributable to FSE.
421. Over time, the agencies should move from inherited FSA settings to an annual property and fleet schedule that records sites, occupancy assumptions, fleet numbers, direct costs, support costs, funding source, review points, and decisions needed for future accommodation, secure storage, public-facing premises, regional presence, and fleet demand.

Roles and responsibilities

- 422. Police is responsible for managing the property, facilities, fleet, supplier, lease, procurement, insurance, asset-system, and finance processes that sit within Police's corporate machinery.
- 423. FSE is responsible for identifying its accommodation, public-facing service, workforce, security, privacy, secure-storage, regional, and fleet requirements, and for advising Police of changes that may affect property or fleet support.
- 424. Both agencies must keep clear the distinction between financial asset and liability management, practical service use, and cost accountability. FSE may define its business need, challenge cost assumptions, seek transparency, and agree funding treatment, even though the Chief Executive may not manage assets and liabilities.

Boundary constraints and limits

- 425. Police property and fleet support enables FSE's Day 1 operations, but it does not give Police control over FSE's regulatory priorities, public-facing service design, regional engagement, or use of funding for statutory functions. Police may apply property, safety, security, procurement, lease, fleet, insurance, and financial controls where needed for lawful administration, probity, auditability, safety, supplier compliance, or protection of public money.
- 426. Those controls should not become de facto approval rights over FSE's operating model. Co-location, shared premises, and shared vehicles may be necessary during transition, but should not obscure FSE's separate statutory identity or lock in inherited FSA settings. Existing sites and vehicles should be tested against actual demand, public-facing identity, privacy, staff safety, secure storage, regional coverage, accessibility, service quality, and value for money.
- 427. Both agencies will identify how continuity will be managed if Police operational priorities, emergencies, major events, or site constraints temporarily affect FSE's access to shared premises, vehicles, secure spaces, or facilities support.

Cost, demand and service standards

- 428. Property and fleet costs should be transparent and matched to the service provided. Direct costs should be identified separately from baseline host capability, and fleet charges should distinguish lease, running, insurance,

maintenance, booking, fuel, telematics, administration, and accident-related costs where relevant.

429. The transition-year funding model should use current FSA arrangements as a starting point only. It should continue clearly attributable property and fleet charges where they are already operating, but require evidence for any additional or changed costs caused by the autonomous agency model.
430. Where FSE uses existing Police space and Police's cost base does not materially change, new broad overhead charges should not be assumed unless an agreed cost-sharing basis is identified. Where FSE requires dedicated premises, additional space, fit-out, secure storage, facilities support, or allocated vehicles, those costs may be treated as direct, incremental, pass-through, or transition costs depending on their nature.
431. Service standards should be realistic for the transition year and delivered through existing Police service channels, suppliers, and relationship leads, with clear escalation where supplier, lease, site, fleet, safety, privacy, or operational pressures affect delivery.

Main risks

432. The main delivery risks are that inherited FSA premises and fleet settings are rolled forward by default, become embedded before demand is understood, or create a public-facing identity that does not support FSE's autonomous regulator role. There is also a risk that fleet size, vehicle type, location, or utilisation does not match actual regulatory demand once the model is operating.
433. Reviews should focus on whether premises and fleet arrangements remain necessary, proportionate, safe, privacy-appropriate, cost-visible, and aligned with FSE's public-facing service model.

Transitional issues and interim solution options

434. The immediate transition issue is Day 1 continuity while FSE's longer-term footprint, operating model, public-facing service design, workforce profile, fee settings, and funding arrangements mature. The transition-year model should prioritise continuity, safety, transparency, and reviewability over false pricing precision.

435. For the transition year, Police should continue to manage the property, lease, facilities, fleet, supplier, insurance, procurement, and finance machinery where those arrangements sit within Police. FSE should fund or contribute to clearly attributable property and fleet costs that support its statutory functions, but those costs should be documented, evidenced, classified, and reviewed.
436. Quarterly reviews should test occupancy, fleet use, direct costs, service issues, privacy and safety issues, demand changes, and unresolved assumptions. A Year 1 wash-up should inform the Year 2 property and fleet schedule, including any baseline transfer, direct cost pass-through, fleet lease reset, footprint change, or staged maturity plan for premises, secure storage, regional coverage, fleet demand, supplier options, and enduring funding treatment.