PUBLIC SAFETY NETWORK
TE KUPENGA MARUTAU

Public Safety Network

Appendix 5.2

Functional Guidelines Test Strategy Outline

Commercial In Confidence

Contents

1. Introduction

The Public Safety Network (PSN) programme is an Emergency Services initiative on behalf of Fire and Emergency New Zealand (Fire and Emergency), New Zealand Police (Police), St John New Zealand (St John), and Wellington Free Ambulance (WFA). The PSN programme is tasked with delivering Mission Critical communication services to the Emergency Services sector.

This document should be read in conjunction with the *Appendix 1. Service Requirements* and *Appendices 4.1 to 4.5 Services Guideline* documents.

2. Document Purpose

This document is part of the Acceptance workstream. It is intended to provide a high-level view of the programme's approach to testing, which includes:

- The types of testing required;
- Test roles and responsibilities;
- Test artefacts;
- Test governance;
- Defect management; and
- Test environments.

2.1 Test Strategy Overview

The Acceptance workstream and PSN Test Strategy will ensure that:

- The PSN services meet agencies' operational needs and align with benefits realisation plans;
- Service and business requirements are met;
- Services comply with relevant national and international standards; and
- Devices are fit-for-purpose.

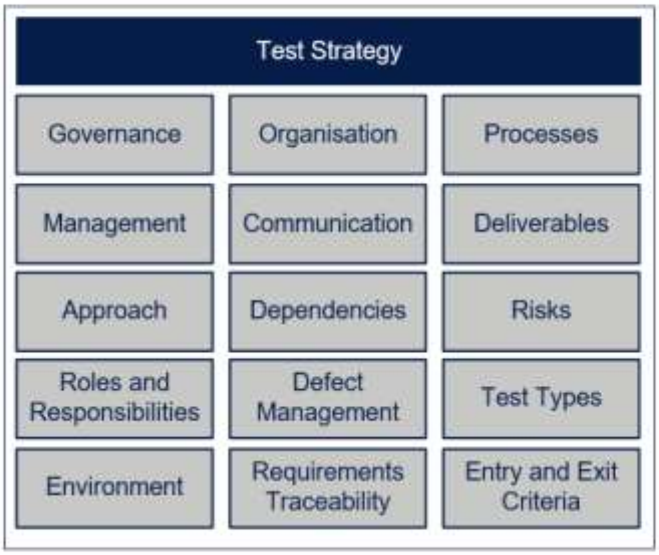
Delineation of responsibilities between Service Providers, delivery partners and agencies will ensure that testing of proven technologies and services will be avoided, especially where common consumer capability forms part of a PSN service.

Emergency Services agencies will need to verify, validate, and pilot the PSN services to ensure that they meet the agencies' requirements and operational needs. This Test Strategy document will guide the processes and approaches that will be taken to ensure that the PSN communications capability aligns with the standards required for the Emergency Services. It will provide stakeholders with a common understanding of the following objectives:

- Identify testing processes;
- Describe the test governance framework;
- Describe test types and approaches to be employed;
- Describe stakeholder engagement and coordination;

- Describe criteria used to determine test entry and exit;
- Describe test deliverables;
- Identify, document, and communicate test-related risks, dependencies, assumptions, and constraints;
- Identify test roles and responsibilities;
- Describe the type of test environments needed to support the planned test effort;
- Describe a defect management process to support testing;
- Describe communications and reporting requirements; and
- During the testing phase, identify any flaws or gaps in the testing strategy or processes that need to be remedied before completed and ongoing testing can be signed off.

The components that make up this Test Strategy are shown below:



Test Strategy		
Governance	Organisation	Processes
Management	Communication	Deliverables
Approach	Dependencies	Risks
Roles and Responsibilities	Defect Management	Test Types
Environment	Requirements Traceability	Entry and Exit Criteria

Figure 1: Test strategy components

2.2 PSN Acceptance Participants

The following parties have a role in the Acceptance workstream:

The PSN programme	• Responsible for end-to-end testing and acceptance of the capability reporting to the Programme Control Board • Manages the Acceptance workstream
Service Providers	• Responsible for testing of services, equipment, devices and resolution of defects, configuration, and compatibility issues • Supports the wider Acceptance workstream

Delivery partners	• Manage delivery of services to the PSN programme. Responsible for the testing of those services
Emergency Services agencies	• Establish transition projects to adopt PSN services. These projects will have associated test activities from test planning for transition through to production acceptance

3. Test Overview

3.1 Test Governance Lifecycle

Test Governance is the set of processes and responsibilities that enable control and co-ordination of test processes across test phases. The test phases (the test lifecycle) provide a management framework to ensure that quality is retained throughout the process, from planning through to production, and that PSN services meet agency expectations.

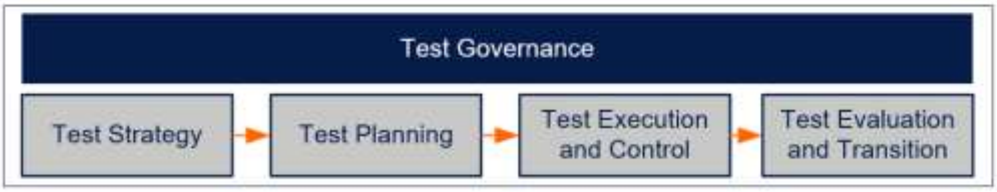


Figure 2: Test governance lifecycle

3.1.1 Test Strategy

During the Test Strategy phase, the programme's test and acceptance strategy is established and test practices and methodologies are defined to allow stakeholders to gain a clear understanding of the test approach.

3.1.2 Test Planning

During the Test Planning phase, project Test Plans will be established that include test scope, the types of testing required, test management approaches, test resources, and test environments. Test Planning also includes deliverables, acceptance criteria, quality standards, schedules, roles and responsibilities, Test Plans, and the verification and validation approach.

3.1.3 Test Execution and Control

The finalised project Test Plans and processes are implemented. Measurement tools are set up, and test governance processes are implemented. Problem tracking and reporting tools are established.

Test Managers monitor testing, including:

- Ensuring the completion and correctness of test cases;
- Ensuring the team is providing consistent documentation for defect and test execution reporting;
- Ensuring the test environment and test data are ready for execution;
- Monitoring the test execution process;
- Managing the defect management process; and

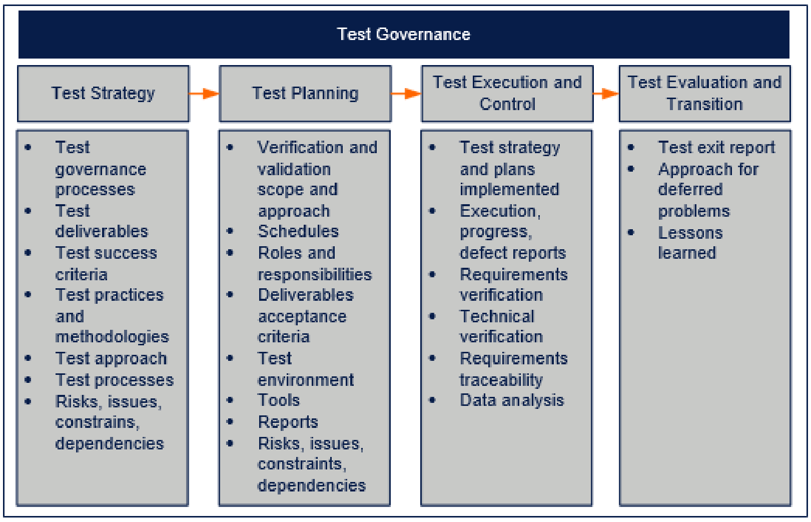
- Conducting quality checkpoints.

3.1.4 Test Evaluation and Transition

In the Transition phase, a Test Exit Report is created and conclusions from test execution are summarised. Other deliverables include lessons learned documentation and an agreed approach for managing any deferred defects.

3.1.5 Test Deliverables

The deliverables associated with test lifecycle are laid out below:



Test Governance

Test Strategy → Test Planning → Test Execution and Control → Test Evaluation and Transition

Test Strategy	Test Planning	Test Execution and Control	Test Evaluation and Transition
• Test governance processes • Test deliverables • Test success criteria • Test practices and methodologies • Test approach • Test processes • Risks, issues, constrains, dependencies	• Verification and validation scope and approach • Schedules • Roles and responsibilities • Deliverables acceptance criteria • Test environment • Tools • Reports • Risks, issues, constraints, dependencies	• Test strategy and plans implemented • Execution, progress, defect reports • Requirements verification • Technical verification • Requirements traceability • Data analysis	• Test exit report • Approach for deferred problems • Lessons learned

Figure 3: Test deliverables/lifecycle

3.2 Test Governance Organisation

This section outlines the proposed high-level testing organisation structure. Emergency Service agencies will establish projects to transition to the PSN services. Test Managers for these projects will oversee the testing outcomes and deliverables required from the projects. Programme Test Management will work closely the Test Managers to align the scope, schedule, cost, quality, resources, communications, and risks. This approach will allow the Programme Control Board to have a consolidated view of plans, management, risks, status, progress monitoring, and control.

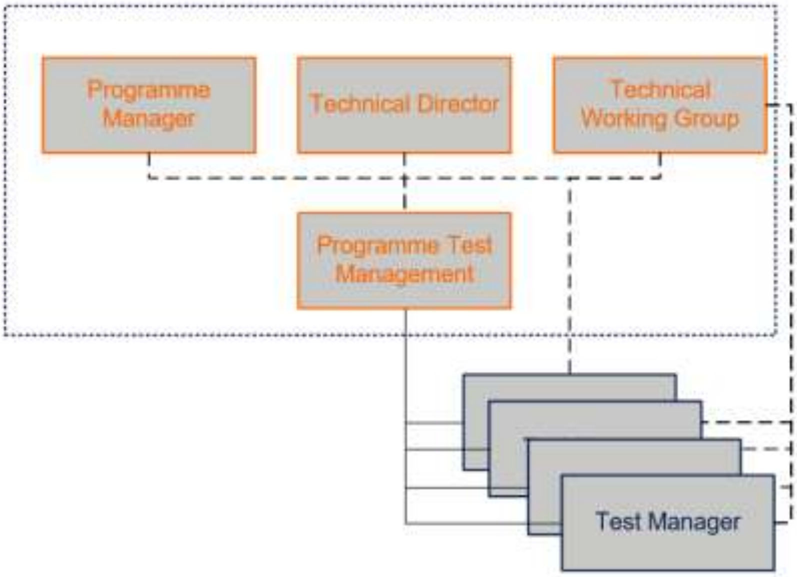


Figure 4: PSN Programme and Test Managers

Programme Test Management will:

- Define and execute the PSN Test Strategy;
- Oversee the test activities across different parties where required;
- Be responsible for any test outcomes directly owned by the PSN programme;
- Participate in services performance evaluation;
- Monitor testing activities, test results, defects, root cause analysis and identify areas of improvement;
- Provide a consolidated view of test monitoring and control across multiple projects; and
- Gather and present consolidated testing metrics and testing activities to the PSN and the Programme Control Board.

Delivery partner, PSN and agency Test Managers are responsible for the effective management of test activities for the projects that they are assigned to. Their primary accountabilities are:

- Define, manage and implement the project test strategy and approach;
- Manage the implementation and adherence to testing methods and standards;
- Help projects achieve their objectives by ensuring that testing requirements are scoped, planned, and managed effectively;
- Develop test plans and assist in the production and review of all test deliverables;
- Ensure that test environment requirements are clearly documented and agreed;
- Execution of test scripts;
- Logging and management of defects;

- Produce metrics to measure test quality and progress;
- Highlight and manage risks, issues, and assumptions identified during Test Planning, test design and execution;
- Work closely with PSN programme Test Management and Service Providers to clarify test requirements throughout the test lifecycle; and
- Responsible for final sign-off of testing prior to production implementation.

3.3 Test Management

Test Management is the implementation of coherent test processes to oversee testing activities, as well as alignment with overall programme goals. These processes are related to:

- Alignment with PSN Test Strategy;
- Test planning;
- Test execution and control; and
- Test evaluation and transition.

3.3.1 Test Planning

The output of test planning is the Test Plan, which defines test scope, confirms the Test Management approach, outlines the types of testing required, confirms test acceptance criteria, and identifies test resources including test environments – the 'How, Who, When and Where'. The Test Plan also establishes the processes for monitoring, control, and reporting. There will be multiple Test Plans across the Emergency Services agencies, the PSN programme, delivery partners and Service Providers.

3.3.2 Test Execution and Control

3.3.2.1 Test Analysis and Design

Test analysis is the process of analysing business and technical documentation and working with business and technical experts to define the test objectives.

Test design addresses how a requirement, function or process will be tested by identifying the test cases that will be performed to verify the implementation of a specific requirement, function or process.

3.3.2.2 Test Execution

Test execution is the process of running a test on the service, capability or function under test and producing a test result. The main outputs of test execution are:

- Executed test cases (or test execution logs);
- Defect reports; and
- Test Status Reports

3.3.2.3 Test Control

Test Control is the ongoing activity of comparing actual progress to the Test Plan and schedule and reporting test status, including any deviations from the plan. It also involves taking any control or corrective actions necessary to meet the project's objectives. Test control guides test through each of the test types to fulfil the test process objectives.

During test design and execution, the Test Manager's role is to:

- Monitor progress according to the plan;
- Initiate and carry out control and corrective actions;
- Ensure Test Status Reports provide an accurate record of test status and progress; and
- Ensure traceability between tests, defects, and requirements is maintained.

3.3.3 Test Evaluation and Transition

The Test Manager will issue a Test Exit Report, summarising the test activities performed for the project, detailing test results (a status of test cases and their parent requirements and a defect summary), assessing test exit criteria, and listing all deviations from the Test Plan. The Test Exit Report is a key communications deliverable for stakeholders, business representatives, and project team members with the aim of obtaining agreement, support, and signoff from the relevant parties. The report provides all the relevant information for stakeholders to make an informed decision regarding suitability of the service, capability or function for production use.

Once test execution is complete the Test Manager will perform the following activities:

- Test completion check - ensure that all test work has concluded;
- Test artifacts handover - provide work products to stakeholders;
- Lessons learned - retrospective meetings where important lessons are captured to inform future projects or test exercises; and
- Archive results, logs, reports, and other documents.

3.4 Communications Management

Key stakeholders for test communications include the following roles and functions:

- PSN Programme Manager;
- PSN Technical Director;
- PSN Technical Working Group;
- Agency Projects Boards;
- Agency Projects, Business, and Technical Managers;
- Agency Technical Stakeholders;
- Agency Business Stakeholders; and
- Agency Test Managers and Testing Teams.

3.5 Requirements Traceability

A Requirements Traceability Matrix will be established to map the service requirements, Test cases and test results to ensure that all requirements have been addressed during the verification and validation process.

The purpose of the Requirements Traceability Matrix is to:

- Provide an overall view of requirements and their test approach;
- Show how requirements are linked to test cases;
- Ensure requirements coverage; and
- Depict the quality status of the requirements by highlighting the test pass/fail percentages and defect density for each requirement.

It will show linkages between:

- PSN Aggregated Service Requirements;
- Agency specific requirements;
- Technical Specifications;
- Test cases;
- Test Execution Status; and
- Defects.

3.6 Change Management

Changes to service requirements, technical specifications and designs could impact the test lifecycle from planning through to execution. These changes could also lead to invalidation of earlier test results or may result in significant deviation from the baseline Test Plan and approach.

The Acceptance workstream and Test Management will be reviewers in the programme and project change management processes. Programme Test Management or the relevant Test Manager will assess any change requests to confirm the impact on the Test Plan, including approach, schedule, cost, scope, risks, and benefits.

Following approval or rejection of the change request the Test Plan and processes will be updated.

4. Testing Types

A set of comprehensive acceptance test procedures will be developed to ensure compliance with service requirements, agency specific requirements and industry standards. These will detail specific test and measurement parameters and will provide the means to verify all requirements. Specific tests will be identified at programme and project levels, including the details of what tests are to be performed, who performs the tests, the parameters to be tested, where the tests will be conducted, the data to be recorded, and when the tests will be conducted.

The testing types include the following:

1. Factory testing;
2. Network testing;
3. Coverage testing;
4. Failure mode testing

5. Performance testing;
6. Security testing;
7. Usability testing;
8. Certification and Service Level Agreements inspection;
9. System testing;
10. System integration and network interworking testing;
11. Operational testing by users;
12. Interoperability testing; and
13. Inter-regional communications testing.

4.1 General Principles

The principles of the agency and delivery partner acceptance testing process will include:

1. PSN shall have the right to review for completeness and approve all Service Provider test and certification procedures.
2. PSN shall have the right to have a representative present to witness Service Provider testing, re-testing, and/or inspections.
3. PSN will perform independent tests to confirm solution conformance to business requirements.
4. Any test/inspection that fails shall be documented, and a resolution plan will be devised.
5. All tests shall be conducted utilising equipment representative of equipment that will be deployed throughout the network.
6. Service Providers will be accountable for correcting any test/inspection failure, and repeating the failed test/inspection.

4.2 Factory Testing

Factory testing ensures that equipment meets the minimum required level of specification. Service Providers must provide factory test results for all equipment (subscriber radios, network infrastructure, etc.) that will be provided as part of the PSN communications capability, including interfaces. This testing includes technical parameters and both functional and operational tests.

Factory testing covers the full hardware and software functionality of all equipment. Testing is completed using the equipment integrated as it will be implemented in the field. Acceptance only be granted after PSN has received all test results and has verified that the equipment has passed all specific tests. PSN may also choose to witness some or all factory tests.

4.3 Network Testing

Network testing provides an objective, independent view of the network to provide assurance that the risks of network implementation have been adequately addressed. System network testing will be carried out by the Service Providers in the lab to validate and bench-test network elements before they are implemented to production. PSN may request access to the network lab to apply functional and performance tests to the network elements whilst they are available. Following lab testing the Service Providers will repeat network testing for each area covered during the capability roll-out. Service Level Agreements for guaranteed quality of service, priority, and pre-emption capability are in the scope of network testing.

4.4 Coverage Testing

Coverage validation requirements and methodology will be covered in *Appendix 5.1 Functional Guidelines Coverage.*

4.5 Failure Mode Testing

The backbone network (e.g., microwave system, leased lines, etc.) and the Land Mobile Radio system, collectively the infrastructure, are required to survive various degrees of failure of system components, including, but not limited to: individual base station/repeater failure, system switch failure, and trunking control channel interference. The Service Providers will document these and other failure modes and describe all the failure recovery modes inherent in the proposed infrastructure.

The Service Provider will simulate each of these failure modes as part of failure mode testing and demonstrate successful failure recovery. As a further part of failure mode testing, automatic alarm reporting will be demonstrated, and service and network management processes will be tested.

Devices and accessories use a diverse range of technologies to collect information, communicate with each other, and transmit data to other devices and computer systems. Due to the mix of different devices, platforms, protocols, and communication gateways, systems often suffer from potential performance, reliability, interoperability, and scalability problems. Service Providers need to test devices to verify that they are working as per specifications under various failure conditions.

4.6 Performance Testing

Service Providers will provide performance testing results to verify that the solution meets the non-functional requirements for performance. This is critical to ensure that the system data flow and processing is occurring within acceptable thresholds to allow for safe and effective responses.

Performance testing demonstrates how devices, networks, software and internal and external applications are functioning to achieve performance objectives. It determines a wide range of parameters, including execution flows, timing, response times, reliability, and stability. It also checks usability, customer satisfaction and how well a system is meeting Service Level Agreements. In addition, scalability testing establishes how adding more devices and workload could affect system performance, responsiveness, and stability.

Performance testing should look at three main levels:

- System level: processing, analytics, database, etc;
- Application level; and
- Network and gateway level.

The tests can, for instance, establish the ability of the embedded software to perform the required computations or the reliability and stability of communication networks under certain operational conditions.

Performance testing will also verify the ability of the solution to scale to accommodate other agencies in the future.

4.7 Security Testing

Best-practice guidelines for network security will be applied to protect the network against threats such as denial-of-service attacks. Access, integrity, and confidentiality controls will include mutual authentication between the network and user devices, and encryption of the control-plane and user-plane traffic. Tests for vulnerabilities in radio frequency (RF) networks, looking at Wi-Fi, cellular, and radio systems may also be applied.

The security of devices shall be assured by a combination of access controls, such as:

- Passcode access; or
- Device hardening (e.g disabling unused services);
- Security applications and settings (such as end-point protection and centralised configuration management); and
- Over the Air control (such as standardised build-and-application set, remote disable and wipe capability).

4.8 Usability Testing

Usability testing establishes whether devices and services are suitable for their application and easy to use. It looks at the end-user experience, including the functionality of all features. Factors to consider include portability and the ability to capture and send notifications, as well as error messages when the device encounters problems.

Depending on device design, the test may verify its ability to collect and process information within the device or in external systems. It also ensures that it can display clear information on mobile devices or computers.

4.9 Certification and Service Level Agreements

The Service Provider will provide certification or qualification certifying that a product, service or capability has passed performance tests and quality assurance tests, and meets the qualification criteria and Service Level Agreements stipulated in any applicable contracts, regulations, or specifications.

The Service Provider needs to submit the results of their conformance and compliance testing for devices and equipment. For network features, Service Providers will need to provide confirmation of the Service Level Agreement (SLA) (e.g. conformance to 3GPP defined Mission Critical and Quality of Service, pre-emption, and priority access to the network).

4.10 System Testing

System testing will be conducted by all Service Providers to ensure that system components and internal integrations between software and hardware are functioning as expected and have been built as specified based on business requirements and design.

Evidence of system testing must be provided by the Service Provider highlighting test coverage, test results, and any outstanding issues.

4.11 System Integration Testing

The purpose of System Integration Testing is to ensure that integrated systems, interfaces, network interworking and associated data flows are working as expected based on the solution requirements and design. This may include data validation testing, end-to-end process testing, two-way data transactions and other activities designed to exercise the integration points of the solution in a production-like (‘real-world’) manner.

Where test environment integration is limited, stubs or other simulated components may be utilised, however the preference is to conduct System Integration Testing in a fully integrated test environment whenever possible.

The tests verify that the systems will produce results in a standard format that users and applications can access, regardless of the make and model of the user interface device, type, and version of operating systems.

4.12 End-to-End Testing

Wherever possible, operational testing should be carried out in an end-to-end test (pre-production) environment prior to implementation into an operational or production environment. End-to-end testing will validate and verify whether the flow of a service, system or function, from start to finish, is behaving as expected.

End-to-end testing may be carried out in a production like environment (a controlled production environment may mean specific cell towers and stations in certain areas).

The purpose of performing end-to-end testing is to validate that system dependencies behave as expected and to ensure that the data integrity is maintained between various system components and systems.

In end-to-end testing real system components and devices will be used instead of mock-ups and stubs and techniques like Field and Drive Testing will be applied. This means that production-like data will be sent.

End-to-end testing will confirm that the solution is fit-for-purpose after implementation of products, equipment, and network devices.

4.13 Operational Testing

Agencies will conduct testing on a pilot system and verify the functionality of all equipment and systems deployed in the field. Service Providers will provide support for all pilot testing. Major elements of the system include, but are not limited to, the following:

- Telecommunication backbone network tests;
- Land Mobile Radio system tests (portable, mobile, control station);
- Mission Critical Push-to-Talk (Cellular) tests;
- Cellular priority and pre-emption tests;
- Personal Alerting; and
- Satellite tests.

The Service Providers will be responsible for the end-to-end performance of the network.

Selected Emergency Services agency personnel will be issued subscriber units to perform functionality tests using portable radio units, consoles, and vehicles (including marine and air) with installed subscriber voice and data terminal devices. The operational system testing shall proceed with sufficient qualities to demonstrate actual working conditions and the environment. Testing will include interface testing to external systems (i.e. data servers, sites, or systems). Performance will be monitored, including:

- Reported poor coverage areas;
- Reported poor audio quality;
- Reported poor data performance;
- System/channel uptime and overall performance; and
- User and application response times.

Operational testing will be conducted by each agency using test cases or scenarios based on real-world business processes. This testing is intended to validate that the solution is fit-for-purpose, meets business expectations, supports business processes, and has a suitable level of usability for the target user group. The outcomes of this testing will be used to determine formal business acceptance of the solution prior to deploying to production.

4.14 Interoperability Testing

Interoperability testing will also be included to verify the ability of new services to interface and communicate to legacy services, other new services, and Command and Control Centres. Any inter-agency communication scenarios should also be tested.

4.15 Inter-Regional Communications Testing

This will also include tests of inter-regional communication with other systems through appropriate gateway interfaces. This assesses how well combining a wide range of devices using different interfaces, network topologies, and protocols will work together and allow the exchange of data across platforms and devices.

4.16 Test Types for Service Categories

The following section outlines and defines the types of testing that will be conducted for the different service types:

	Factory Testing	Network Testing	Coverage Testing	Performance Testing	Security Testing	Usability Testing	Certification and SLA	Failure Mode Testing	System Testing	System Integration Testing	End to End testing	Operational Testing
Cellular Services		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Mission Critical PTT		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Digital LMR		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Devices and Accessories	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Device and Application Management					Y		Y	Y	Y	Y	Y	Y
Transparent Network Management							Y	Y	Y		Y	Y
Vehicle and Coverage Solutions	Y		Y	Y	Y		Y	Y	Y	Y	Y	Y
Personal Alerting		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Satellite Services			Y			Y					Y	Y

4.17 Service Provider/PSN Test Delineation

Test Type	Service Provider Responsibility	PSN / Agency Responsibility
Overall	The overall design, requirements, performance expectations, guarantees, interface requirements, compliance with standards. Testing of services, equipment, devices. Resolution of defects, configuration, and compatibility issues.	Service and business requirements. Technical specifications. Inspection and testing.
Cellular Services	Mobile coverage maps, coverage guarantees. Countrywide coverage proof of performance drive test including signal measurement and voice quality. Evidence of testing procedures, and test results including, but not limited to the following: • Network testing; • Coverage testing; • Performance testing; • Security testing; • Certification and Service Level Agreements; • Failure mode testing; • System testing; and • System integration testing.	Testing of the agency business and technical requirements. • Operational testing; and • Inspection/audit of Service Provider's test procedures and Service Level Agreements.
Mission Critical Push-to-Talk	Evidence of testing procedures, and test results including but not limited to the following: • Network testing; • Coverage testing; • Performance testing; • Security testing; • Certification and Service Level Agreements; • Failure mode testing.	Testing of the agency business and technical requirements: • Operational testing; • Usability testing; and • Inspection/audit of Service Provider's test procedures and Service Level Agreements.

	• System testing; and • System integration testing.	
Digital LMR	Evidence of testing procedures, and test results including but not limited to the following: • Network testing; • Coverage testing; • Performance testing; • Security testing; • Certification and Service Level Agreements; • Failure mode testing; • System testing; and • System integration testing.	Testing of the agency business and technical requirements: • Operational testing; and • Inspection/audit of Service Provider’s test procedures and Service Level Agreements.
Devices and Accessories	Evidence of testing procedures, and test results including, but not limited to the following: • Failure mode testing; • Coverage testing; • Performance testing; • Security testing; • Usability testing; • Certification and Service Level Agreements; • Failure mode testing; • System testing; and • System integration testing.	Testing of the agency business and technical requirements: • Operational testing; • Usability testing; and • Inspection/audit of Service Provider’s test procedures and Service Level Agreements.
Device and Application Management	Evidence of testing procedures, and test results including, but not limited to the following: • Security testing; • Certification and Service Level Agreements; • Failure mode testing; • System testing; and	Testing of the agency business and technical requirements: • Operational testing; • Usability testing; and • Inspection/audit of Service Provider’s test procedures; and

	- System integration testing.	Service Level agreements.
Transparent Network Management	Evidence of testing procedures, and test results including, but not limited to the following: - Certification and Service Level Agreements; - Failure mode testing; - System testing; and - System integration testing.	Testing of the agency business and technical requirements: - System integration testing; - Operational testing; - Usability testing; and - Inspection/audit of Service Provider's test procedures and Service Level Agreements.
Vehicle and Coverage Solutions	Portable are coverage probability maps, coverage area availability guarantees: - Factory testing; - Coverage testing; - Performance testing; - Security testing; - Certification and Service Level Agreements; - Failure mode testing; - System testing; and - System integration testing.	Testing of the agency business and technical requirements: - Operational testing; - Usability testing; and - Inspection/audit of Service Provider's test procedures and Service Level Agreements.
Personal Alerting	Evidence of testing procedures, and test results including, but not limited to the following: - Network testing; - Coverage testing; - Performance testing; - Security testing - Certification and Service Level Agreements; - Failure mode testing; - System testing; and	Testing of the agency business and technical requirements: - Operational testing; and - Inspection/audit of Service Provider's test procedures and Service Level Agreements.

	• System integration testing.	
Satellite Services	Evidence of testing procedures, and test results including, but not limited to the following: • Usability testing • Certification and Service Level Agreements.	Testing of the agency business and technical requirements: • Operational testing; and • Usability testing. Inspection/audit of Service Provider's test procedures and Service Level Agreements.

5. Assumptions and Dependencies

The following section outlines testing related assumptions and dependencies.

5.1 Assumptions

The PSN Test Strategy has been created using the following assumptions:

- Service Providers are accountable for the testing, performance, and quality of provided products and services. Agencies will perform integration testing of their systems and operational testing and end-to-end testing of business processes.
- Service Providers will provide SLAs, certifications, and test procedures that can be used as success criteria for some of the agency's test objectives. This should be detailed in the agency's Test Plans.
- The test team will have access to PSN working groups for business and technical queries.
- Test environments will be built to enable integration and operational testing.
- Technical experts from the Service Providers' development and technical teams will be available to assist and resolve any queries during test case/script development, test execution, and result validation.
- Each agency will perform operational testing using their internal test team, which will include business Subject Matter Experts and business users.

5.2 Dependencies

Testing is dependent on:

- Set-up of appropriate test environments;
- Builds being available and ready for the tests on time on the right environment;
- Test data being available before starting test execution;
- Software and hardware integration testing of services being completed, tested and validated by the Service Provider; and
- Inter-agency testing which will require close co-ordination of schedule and resources.

6. Risks

Below is the list of testing-related risks involving Service Providers.

#	Risk Statement	Mitigation
2	If the technical solution does not meet the agencies’ requirements, then the solution may not be fit-for-purpose.	• Extensively engage with the Service Providers’ technical teams to define a quality assurance, and defect management process. • Use an effective test organisation structure and controls for seamless communication and prioritisation of issues. • Establish a defect management group made up of business and technical stakeholders for clarification on requirements. • Establish an effective change and configuration management process for implementing fixes. • Ensure that the resources needed for issue resolution are available as needed. • Place contractual obligations on Service Providers.
7	If the test environment is not established in time, then testing could be delayed.	• Engage with the Service Providers’ and the agencies’ technical teams to define test environment requirements. • Detail the test environment requirements in the Test Plan. • Engage with technical teams to set up the test environment and test data.

7. Defect Management

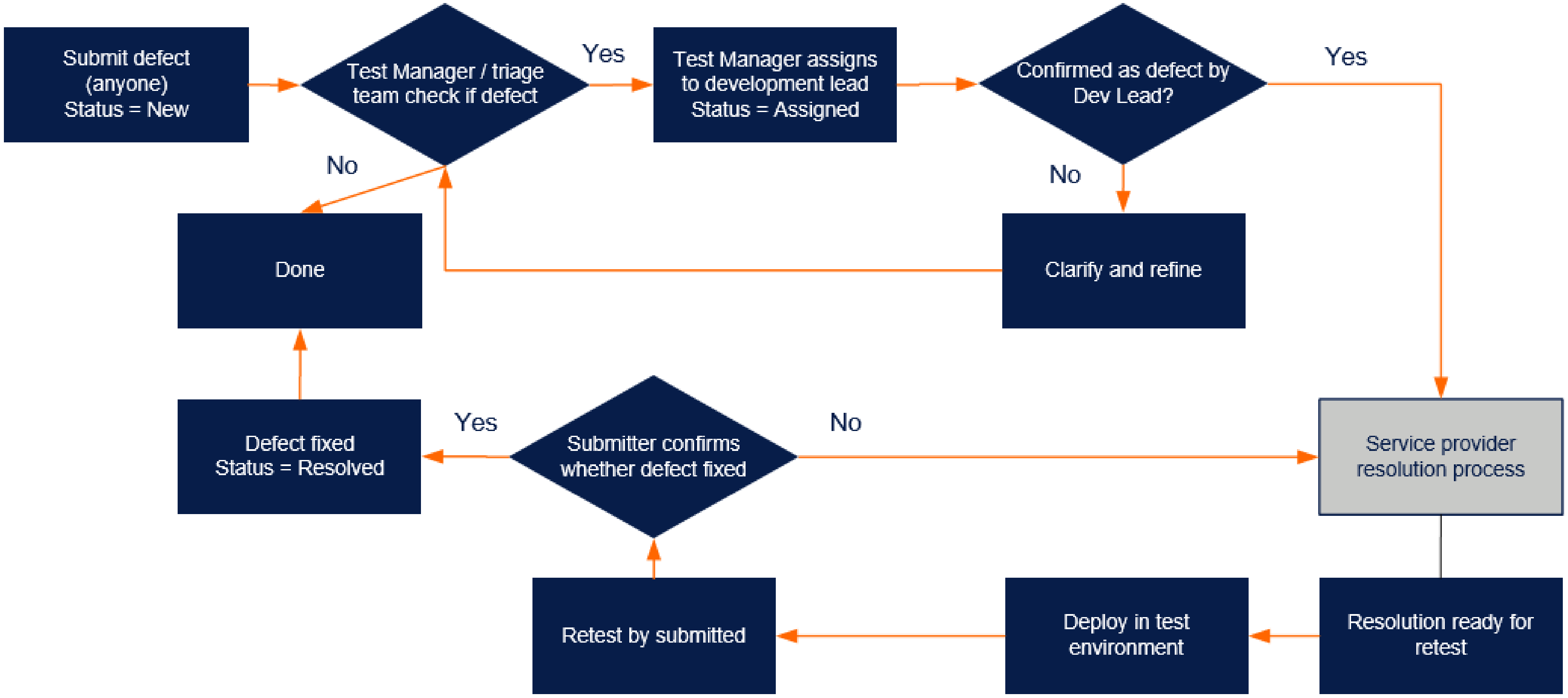
Defect management will be co-ordinated by the Test Manager and will involve communication and collaboration across the project team and Service Provider teams.

Regular defect review/triage meetings will be held regardless of the specific Service Providers or services involved.

This section details the proposed general processes and standards for defect management during testing phases. It is expected that a multi-agency approach for defect management will be established and detailed in Test Plans.

7.1 Defect Workflow

The following diagram outlines a general defect workflow.



Submit defect (anyone) Status = New
Test Manager / triage team check if defect
Yes
No
Test Manager assigns to development lead Status = Assigned
Confirmed as defect by Dev Lead?
Yes
No
Done
Clarify and refine
Defect fixed Status = Resolved
Yes
Submitter confirms whether defect fixed
No
Service provider resolution process
Retest by submitted
Deploy in test environment
Resolution ready for retest

8. Test Environments

This section is intended to provide a high-level explanation of the environments required to support the testing activities.

A test environment is a combination of hardware, software, data, and configuration that is required to execute testing. Each service type or test type might need a different or modified version of a test environment. The test environment set-up would depend upon the service type, test level, and business process under test.

Detailed test environment requirements will be described in the relevant Test Plans. A review of the test approach and technical architecture will formulate an understanding of the general environment needs for the testing effort. General steps followed for test environment configurations will be:

- Review test approach, test type, service being tested, and technical architecture diagram;
- Identify the number of different deployment configurations, and review the deployment model;
- Identify each specific test configuration and environment that software and hardware will be deployed on;
- Consolidate a list of test environments that will provide the broadest range of test coverage;
- For each test environment, collate a list of hardware and software needed for testing;
- Define each test configuration with assistance from technical teams; and
- Define the test environment management process for each environment.

Changes are usually deployed through different environments before going live in production. A typical environment structure includes a development, staging, and production/live environment.

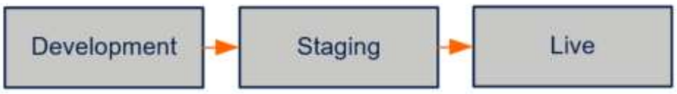


Figure 5: Example environments

8.1 Development Environment

A development environment is used to develop, configure, and test a specific part of a software or hardware. The purpose of a development environment is to enable technical and testing teams to make continuous changes without affecting the end-to-end staging environment where operational testing is carried out.

This environment will be built and used by Service Providers during the development of the solution. The development environment may be a lab and simulators in the case of network testing, and conformance and compliance testing for devices and equipment. Code for software solutions will be deployed, unit tested, then system tested within this environment prior to being deployed to the agencies' test environments for operational testing.

The agencies may choose to set up their own development environments if needed to test agency specific configurations, components, and data in isolation before deploying the solution to the end-to-end staging for further test phases.

It is not expected there will be development or staging environments for validating satellite services.

8.2 End-to-end Staging Environments

The end-to-end staging environment is made, wherever possible, to look exactly like the production environment. The end-to-end solution is tested on the staging environment to check for defects and issues and to ensure it does not fail in the production environment. This type of testing on the staging environment is the final step before the solution can be deployed to a production environment.

The end-to-end staging environment will consist of the various systems, subsystems and components that form the overall solution, represented by a physical test system, to replicate the behaviour and outputs of the real-world system. Details of the specific set-up, configuration, data requirements and other details will be specified in the detailed Test Plans. For example, a staging environment for operational testing shall be established to test the interfaces described in the following figure:

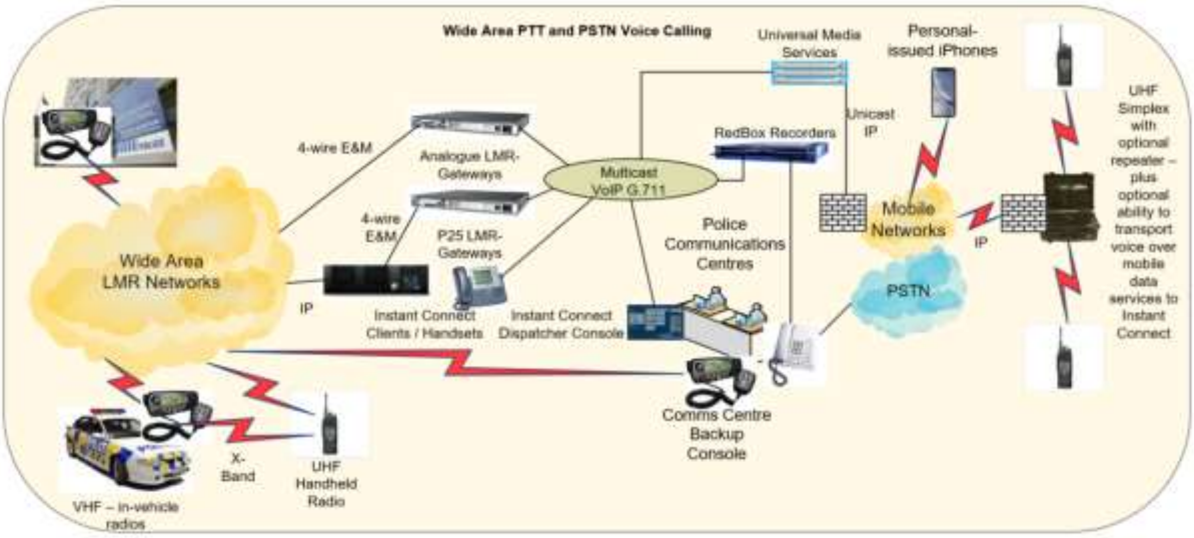

Wide Area PTT and PSTN Voice Calling
Universal Media Services
Personal-issued iPhones
4-wire E&M
Analogue LMR-Gateways
Multicast VoIP G.711
RedBox Recorders
Unicast IP
UHF Simplex with optional repeater – plus optional ability to transport voice over mobile data services to Instant Connect
4-wire E&M
P25 LMR-Gateways
Police Communications Centres
Mobile Networks
IP
Wide Area LMR Networks
IP
Instant Connect Clients / Handsets
Instant Connect Dispatcher Console
PSTN
Comms Centre Backup Console
X-Band
UHF Handheld Radio
VHF – in-vehicle radios

Figure 5: Interface testing

8.3 Cellular, LMR and PTT all require System Integration Testing in Production

The production environment is the fully implemented solution in the real world with the final versions of hardware, infrastructure, network, and code deployed. Agencies may choose to do a pilot run with limited users in this environment to fine-tune the end-to-end solution prior to an agency-wide launch. Any such pilot testing requirements and approaches will be identified during Test Planning.

	Factory Testing	Network Testing	Coverage Testing	Performance Testing	Security Testing	Usability Testing	Certification and SLA	Failure Mode Testing	Operational Testing	System Testing	System Integration Testing
Development Environment	• Devices and Accessories • Vehicles and Coverage	Lab testing for: • Cellular Services • MCPTT • LMR • Devices and Accessories • Vehicles and Coverage	• Cellular Services • MCPTT • LMR • Devices and Accessories • Vehicles and Coverage	• Cellular Services • MCPTT • LMR • Devices and Accessories • Vehicles and Coverage	• Cellular Services • MCPTT • LMR • Devices and Accessories • Vehicles and Coverage • Devices and Application Management	• MCPTT • Devices and Accessories	• Cellular Services • MCPTT • LMR • Devices and Accessories • Device and Application Management • Transparent Network Management • Vehicles and Coverage	• Cellular Services • MCPTT • LMR • Devices and Accessories • Device and Application Management • Transparent Network Management • Vehicles and Coverage		• Cellular Services • MCPTT • LMR • Devices and Accessories • Device and Application Management • Transparent Network Management • Vehicles and Coverage	• Cellular Services • MCPTT • LMR • Devices and Accessories • Device and Application Management • Transparent Network Management • Vehicles and Coverage
Staging Environment		Sample checks for: • Cellular Services • LMR As part of Operational Testing	Sample checks for: • Cellular Services • MCPTT • LMR • Devices and Accessories • Vehicles and Coverage As part of Operational Testing	• Performance Testing scenarios from Operational Testing	• Security Testing scenarios from Operational Testing	• Device and Accessories • MCPTT • Agency Applications and Processes	• Audit of service providers' services, test procedures, certifications and service level agreements	• Cellular Services • MCPTT • LMR • Devices and Accessories • Device and Application Management • Transparent Network Management • Vehicles and Coverage	• Cellular Services • MCPTT • LMR • Devices and Accessories • Device and Application Management • Transparent Network Management • Vehicles and Coverage		• Cellular Services • MCPTT • LMR • Devices and Accessories • Device and Application Management • Transparent Network Management • Vehicles and Coverage
Production Environment		Sample checks for: • Cellular Services • LMR As part of Operational Testing	Sample checks for: • Cellular Services • MCPTT • LMR • Devices and Accessories • Vehicles and Coverage As part of Operational Testing	• Performance Testing scenarios from Operational Testing	• Security Testing scenarios from Operational Testing			• Cellular Services • MCPTT • LMR • Devices and Accessories • Device and Application Management • Transparent Network Management • Vehicles and Coverage	• Cellular Services • MCPTT • LMR • Devices and Accessories • Device and Application Management • Transparent Network Management • Vehicles and Coverage		

The diagram above lists all levels of testing to be performed by different parties including Service Providers, and agency test teams in different test environments.

- **Development Environment**: Testing in this environment will be performed by Service Providers. Factory testing, SLAs and certifications, and network testing will take place in service providers' labs. System testing of software solutions will be completed by Service Providers in this environment as well. The agencies may choose to set up their own development environments if needed to test agency specific configurations, components, and data in isolation before deploying the end-to-end solution to the end-to-end staging environment for further testing. Service Providers will perform production-like testing in their own end-to-end environments or testing sites.
- **End-to-end Staging Environment**: Testing in this environment will be performed by PSN and the Emergency Services agencies. The end-to-end staging environment will allow an opportunity to integrate systems, subsystems, and components from the overall solution represented either physically or virtually to simulate real-world behaviour and outputs. System integration testing for all integrated systems and interfaces will be completed by the agency's test team.
- **Production Environment**: User Acceptance Testing for all system components including software, devices and equipment, network infrastructure, and critical communications feature. A careful selection for a cell tower in low-density areas will allow installing the network and critical communication features in a controlled production environment to complete user acceptance testing.