Penetration Testing Service Definition

Document title	Penetration Testing Service Definition		
Reference No.	IF-SER-032	**Version**	1.0
Author	Lisa Washer, Head of Cyber		
Reviewed by	Holly Jackson, Cyber Manager		
Issue date	23/01/2026		

Document Control

Version	Name	Comment	Date
0.1	Lisa Washer	Initial Draft	07/01/2026
0.2	Holly Jackson	Review and amendments	15/01/2026
1.0	Lisa Washer	Final review and publish	23/01/2026

Correlation Chart

Clause	FSR Code of Practice v2	ISO/IEC 17025:2017	ILAC-G19 :06/2022	ISO 9001:2015	ISO/IEC 27001:2022
Review of Requests, Tenders and Contracts	16	7.1	4.1, 4.7	8	4.2

Penetration Testing Service Definition

Contents

1. Penetration Testing Services

1.1 Service Overview

1.1.1 The Penetration Testing Service provides independent, structured security testing designed to identify and validate technical vulnerabilities across systems, applications, networks, and cloud environments. The service simulates real-world attacker techniques to assess the effectiveness of security controls and identify weaknesses that could be exploited to compromise confidentiality, integrity, or availability.

1.1.2 Testing is delivered by qualified penetration testing specialists operating in accordance with recognised industry standards and methodologies. The service supports security assurance, regulatory compliance, risk management, and continuous security improvement.

1.1.3 The Penetration Testing Service is delivered on an ad-hoc consultancy basis or under an agreed programme of testing. Engagements may be scoped to individual systems or extended across multiple environments, subject to appropriate authorisation.

1.1.4 The Penetration Testing Service may be delivered as a recurring or programme-based service, enabling organisations to undertake more frequent and consistent testing across systems and applications. This approach supports continuous assurance, aligns testing with change cycles, and reduces reliance on ad-hoc, one-off assessments.

2. Service Features

2.1.1 Below is a list of the core capabilities and characteristics of the Penetration Testing Service, describing what is delivered and how the service operates:

a) **Scoping and Test Design** - Collaborative definition of scope, objectives, attack surface, and testing rules to ensure alignment with business and risk priorities.

b) **Infrastructure Penetration Testing** - Security testing of internal and external networks, servers, endpoints, and network services to identify exploitable vulnerabilities.

c) **Application Penetration Testing** - Assessment of web and application interfaces to identify common and advanced application security weaknesses.

d) **Cloud and Platform Testing** - Testing of cloud-hosted environments, configurations, and exposed services within authorised scope.

e) **Threat-Led and Scenario-Based Testing** - Testing aligned to realistic attack scenarios and threat models relevant to the organisation.

f) **Exploitation and Impact Validation** - Controlled exploitation of vulnerabilities to demonstrate real-world impact and risk.

g) **Evidence-Based Findings** - Clear documentation of vulnerabilities, exploitation steps, and supporting evidence.

h) **Risk-Rated Reporting** - Findings prioritised using severity and impact ratings aligned to industry best practice.

i) **Remediation Guidance** - Actionable recommendations to support effective remediation and risk reduction.

j) **Independent Specialist Delivery** - Testing conducted by experienced, independent penetration testing specialists.

k) **Programme-Based and Repeat Testing -** Supports more frequent penetration testing through scheduled or repeat engagements, enabling continuous validation of security controls following system changes, deployments, or remediation activities.

3. Service Benefits

3.1.1 Below is a list of the key outcomes and advantages gained from using the Penetration Testing service:

a) **Realistic Risk Identification** - Identifies vulnerabilities that present genuine exploitation risk rather than theoretical weaknesses.

b) **Independent Security Assurance** - Provides objective, third-party validation of security controls and defensive measures.

c) **Improved Security Posture** - Supports prioritised remediation and continuous security improvement.

d) **Regulatory and Compliance Support** - Assists organisations in meeting regulatory, contractual, and assurance requirements.

e) **Reduced Likelihood of Breach** - Helps identify and address weaknesses before they can be exploited by attackers.

f) **Executive and Stakeholder Confidence** - Delivers clear, risk-focused reporting suitable for technical and non-technical audiences.

g) **Informed Security Investment** - Supports data-driven decisions on security control improvements and resource allocation.

4. Scope of Service

4.1 In-scope activities

4.1.1 The Penetration Testing Service may include the following activities, subject to agreed scope:

a) **Engagement Scoping and Planning** - Definition of scope, objectives, constraints, and authorisation.

b) **Penetration Testing Execution** - Active testing of in-scope systems, applications, or environments using approved techniques.

c) **Vulnerability Identification and Exploitation** -Identification and controlled exploitation of security weaknesses.

d) **Reporting and Findings** - Delivery of technical and executive reports documenting findings and recommendations.

Retesting (Optional) - Validation of remediation actions to address identified vulnerabilities.

4.2 Out-of-scope activities

4.2.1 The following activities are excluded unless explicitly agreed:

a) Denial-of-service or stress testing

b) Remediation or system configuration changes

c) Continuous monitoring or managed security services

d) Testing of third-party systems without authorisation

e) Social engineering or physical security testing

4.3 Assumptions, Constraints and Dependencies

4.3.1 Delivery of the Penetration Testing Service is subject to the following assumptions, constraints, and dependencies, which influence scope, timelines, and outcomes.

a) **Authorisation** - Written authorisation is required confirming permission to test all in-scope systems.

b) **Defined Scope** - Testing is limited strictly to agreed systems, IP ranges, applications, and accounts.

c) **Operational Constraints** - Testing is conducted to minimise disruption but may expose system weaknesses.

d) **Point-in-Time Assessment** - Results reflect the security posture at the time of testing only.

e) **Third-Party Dependencies** - Cloud or vendor-managed environments may impose testing constraints.

5. Onboarding

5.1.1 Onboarding commences upon engagement approval and is designed to ensure safe, controlled, and effective penetration testing aligned to operational and business requirements.

5.1.2 During onboarding, the scope, objectives, attack surface, and rules of engagement are confirmed, including in-scope systems, IP ranges, applications, user accounts, and testing constraints. Written authorisation to conduct testing is obtained prior to any activity commencing.

5.1.3 Testing schedule and timing are agreed during onboarding. This includes confirmation of testing windows, duration, time-of-day restrictions, blackout periods, and any change control or business approval requirements. Where required, testing is coordinated to align with maintenance windows, operational risk tolerance, and system criticality.

5.1.4 Key stakeholders, points of contact, and escalation paths are identified. Communication methods and reporting cadence are agreed, including notification requirements for high-risk findings identified during testing.

5.1.5 Access requirements, credentials, and technical prerequisites are documented and validated in advance to prevent delays. Any dependencies on third parties, cloud providers, or managed service providers are identified, and coordination is initiated where necessary.

5.1.6 Onboarding concludes once scope, schedule, access, and authorisation are formally confirmed, enabling penetration testing activities to proceed as planned.

6. Service Delivery Model

6.1.1 The Penetration Testing Service is delivered using a structured and repeatable methodology aligned to recognised industry standards.

6.2 Engagement Approach

6.2.1 A dedicated penetration testing team is assigned, led by a Test Lead responsible for delivery coordination and quality assurance. Testing is conducted independently and evidence-led, with regular communication throughout the engagement.

6.3 Delivery Phases

6.3.1 The service is typically delivered across the following phases:

a) **Planning and Scoping** - Confirmation of scope, objectives, and rules of engagement.

b) **Testing and Exploitation** - Active testing to identify and validate vulnerabilities.

c) **Analysis and Risk Assessment** - Assessment of exploitability, impact, and risk.

d) **Reporting and Close-Out** - Delivery of findings, recommendations, and close-out briefing.

6.4 Typical Timelines

6.4.1 Timelines vary based on testing scope and complexity:

a) Small Scope: 2–5 days

b) Medium Scope: 5–10 days

c) Large or Complex Scope: 10–20+ days

6.5 Delivery Modes

6.5.1 The Penetration Testing Service may be delivered remotely, on-site, or through a hybrid approach depending on environment sensitivity and access requirements.

7. Support Model

7.1.1 The Penetration Testing Service is supported through defined levels of engagement to ensure appropriate coverage for both ad-hoc testing engagements and programme-based testing delivered on a recurring basis. The support model is designed to provide flexibility, responsiveness, and consistent quality, allowing organisations to scale testing effort and support levels in line with risk, change activity, and business requirements.

7.2 Standard Support

7.2.1 Standard Support applies to the majority of ad-hoc and programme-based penetration testing engagements and is designed to provide structured, predictable delivery during normal business operations. Under Standard Support, penetration testing activities are delivered during agreed business hours by qualified penetration testers using approved methodologies. A named Test Lead is assigned to coordinate delivery, manage scope and scheduling, and provide quality assurance across the engagement.

7.2.2 Standard Support includes management of access and testing prerequisites in line with onboarding agreements, delivery of agreed testing activities, and documentation of identified vulnerabilities with supporting evidence. Risk-rated technical reports and executive summaries are produced, and a close-out discussion is provided to explain findings, clarify risk, and outline remediation considerations. Standard Support is suitable where testing can be planned in advance and does not require accelerated timelines or extended availability.

7.3 Enhanced Support

7.3.1 Enhanced Support is designed for higher-risk, time-critical, or complex penetration testing scenarios, including major system releases, regulatory deadlines, or environments requiring increased coordination and responsiveness. Enhanced Support may involve extended testing windows, including out-of-hours or weekend testing, and accelerated delivery of testing and reporting outputs.

7.3.2 Under Enhanced Support, additional testing resources may be allocated to support parallel testing activities, and more frequent status updates and stakeholder briefings are provided. High-risk findings may be escalated earlier in the engagement to support timely risk management decisions. Enhanced Support also supports priority scheduling within programme-based testing arrangements and closer coordination with change, release, or incident management processes. Enhanced Support is provided subject to resource availability and separate agreement and may apply for all or part of an engagement.

7.4 Escalation Paths

7.4.1 Clear escalation paths are defined to ensure issues affecting delivery, risk, or scope are addressed promptly and appropriately.

a) **Operational Escalation** - Operational issues, including scope clarification, access constraints, scheduling conflicts, or technical blockers, are escalated to the Test Lead. The Test Lead is responsible for coordinating resolution and adjusting delivery plans as required.

b) **Risk and Severity Escalation** - Where critical or high-risk vulnerabilities are identified that present immediate business or operational risk, the Test Lead escalates findings to the client's nominated contact in line with agreed notification procedures.

c) **Service and Delivery Escalation** - Issues impacting timelines, quality, or resource availability are escalated to the Cyber Manager, who is accountable for delivery assurance and remediation planning.

d) **Commercial and Strategic** Escalation - Commercial matters, scope changes, or contractual issues are escalated to the Account Manager, who acts as the primary point of contact for strategic and commercial resolution.

7.4.2 Escalation routes and contacts are confirmed during onboarding and may be updated throughout the engagement to reflect changing requirements.

8. Service Level Agreements

8.1.1 The following service levels describe indicative performance targets for the Penetration Testing Service. These service levels are provided for planning and assurance purposes and do not constitute guaranteed commitments unless expressly agreed in writing.

8.1.2 Where a pre-existing contract, framework agreement, retainer, or programme-based testing arrangement is in place, the service levels defined within that agreement take precedence over the indicative service levels outlined below.

8.2 Engagement Acknowledgement

8.2.1 Initial acknowledgement is provided following receipt of a penetration testing request and confirmation that the request falls within service scope.

a) **Ad-hoc Testing Requests**: Acknowledged within 1 business day

b) **Programme-Based Requests:** Acknowledged in line with the agreed programme schedule

8.2.2 Acknowledgement includes confirmation of request receipt, initial feasibility assessment, and identification of next steps for scoping and scheduling.

8.3 Scoping and Scheduling Commitment

8.3.1 Formal scoping and scheduling commence following engagement acknowledgement.

a) **Standard Engagements**: Scoping and testing schedules are confirmed within 2–5 business days

b) **Enhanced or Time-Critical Engagements:** Scoping and scheduling are prioritised and confirmed as soon as practicable, subject to availability

8.3.2 Testing windows, duration, blackout periods, and operational constraints are documented and approved prior to testing commencement.

8.4 Testing Commencement

8.4.1 Penetration testing activities commence once scope, authorisation, access, and scheduling have been confirmed.

a) **Standard Support:** Testing typically commences within the agreed testing window

b) **Programme-Based Testing:** Testing is delivered in accordance with the agreed testing cadence

c) **Enhanced Support**: Testing may commence within 24–48 hours of authorisation, subject to resource availability

8.5 Availability Windows

8.5.1 Availability commitments are confirmed during onboarding and may be adjusted as engagement requirements evolve.

a) **Standard Availability:** Business hours, Monday to Friday (excluding public holidays)

b) **Extended Availability:** Out-of-hours or weekend testing is available under Enhanced Support and subject to agreement

8.6 Reporting Commitments

8.6.1 Reporting deliverables are provided in line with agreed scope and severity of findings.

a) **Interim Notifications:** High-risk or critical findings are communicated promptly in accordance with agreed escalation procedures

Final Report: Typically delivered within 5 business days of testing completion

b) **Retesting Reports**: Typically delivered within 3–5 business days of retest completion

8.7 Programme-Based Service Levels

8.7.1 For programme-based penetration testing arrangements, service levels may additionally include:

a) Pre-agreed testing cadences (e.g. quarterly, monthly)

b) Priority scheduling within the programme window

c) Consistent tester allocation to support continuity

d) Aggregated or trend-based reporting across test cycles

8.7.2 Programme-specific SLAs are documented as part of the programme agreement.

8.8 Escalation and Priority Handling

8.8.1 Escalation procedures are defined to ensure timely management of issues impacting risk, delivery, or scope

a) **Operational Escalation:** Managed by the Test Lead

b) **Service Delivery Escalation:** Managed by the Cyber Manager

c) **Commercial or Contractual Escalation**: Managed by the Account Manager

8.8.2 Critical findings identified during testing are escalated immediately in line with agreed notification thresholds.

8.9 SLA Exclusions and Limitations

8.9.1 The following are excluded from SLA commitments:

a) Guarantees of vulnerability discovery or exploitation success

b) Remediation implementation or validation outside agreed retesting

c) Delays caused by incomplete access, authorisation, or client-side dependencies

d) Testing disruption caused by system instability or operational constraints

8.10 SLA Review and Adjustment

8.10.1 Service levels may be reviewed and adjusted during the engagement where scope, risk, or delivery conditions change. Any changes to agreed SLAs are documented and confirmed in writing.

9. Roles and Responsibilities

9.1.1 The following roles and responsibilities are defined to ensure effective governance, lawful execution, quality assurance, and clear communication throughout the delivery of the Penetration Testing Service. Clear role separation supports independence of testing, accountability for decisions, and defensible outcomes.

9.2 Account Manager

9.2.1 The Account Manager is responsible for overall engagement governance and commercial oversight. This role ensures the service is delivered in line with agreed contractual terms, scope, and client expectations.

9.2.2 Responsibilities include managing commercial arrangements, confirming engagement scope and service levels, coordinating programme-based testing schedules, and handling commercial or contractual escalations. The Account Manager supports strategic alignment of testing activities but does not influence testing methodology, findings, or risk ratings.

9.3 Service Manager

9.3.1 The Service Manager provides operational oversight and quality assurance across penetration testing engagements. This role is accountable for ensuring delivery aligns with recognised penetration testing standards, methodologies, and internal quality controls.

9.3.2 Responsibilities include overseeing tester allocation, managing delivery risks, approving testing approaches, ensuring consistency across programme-based testing, and reviewing reports for quality and accuracy. The Service Manager manages service-level escalations and ensures corrective action where delivery issues arise.

9.4 Test Lead

9.4.1 The Test Lead is responsible for day-to-day coordination and technical leadership of the penetration testing engagement. This role acts as the primary operational point of contact for the client.

9.4.2 Responsibilities include confirming scope and rules of engagement, coordinating scheduling and access, managing testing activities, and ensuring testing is conducted safely and within agreed boundaries. The Test Lead oversees documentation of findings, supports risk escalation for critical issues, and ensures reporting accurately reflects testing outcomes and limitations.

9.5 Penetration Tester

9.5.1 Penetration Testers are responsible for executing the technical testing activities within the agreed scope.

9.5.2 Responsibilities include conducting manual and automated testing, identifying and validating vulnerabilities, performing controlled exploitation where authorised, and documenting findings with supporting evidence. Penetration Testers operate independently and objectively, following approved methodologies and ethical standards, and do not remediate or modify client systems unless explicitly agreed.

9.6 Client Test Lead

9.6.1 The Client Test Lead acts as the organisation's primary point of contact for the penetration testing engagement and is responsible for internal coordination.

9.6.2 Responsibilities include confirming legal authority to test, approving scope and scheduling, coordinating access and credentials, notifying internal stakeholders of testing activities, and supporting escalation where required. The Client Test Lead ensures organisational readiness and facilitates timely decision-making during testing.

9.7 Client Stakeholders and Subject Matter Experts (SMEs)

9.7.1 Client stakeholders and SMEs provide contextual, technical, and operational information required to support effective testing and interpretation of findings.

9.7.2 Responsibilities include supplying system details, clarifying architecture or application behaviour, assisting with access provisioning, and validating business impact of findings. SMEs are consulted as required but do not influence testing conclusions or severity ratings.

9.8 Legal, Risk, or Compliance Representatives

9.8.1 Where testing supports regulatory compliance, assurance, or legal obligations, legal, risk, or compliance representatives may be involved.

9.8.2 Responsibilities include advising on legal authority, regulatory requirements, data handling considerations, and disclosure obligations. These representatives may review reports for compliance purposes but do not direct testing methods or alter technical findings.

9.9 Role Interaction and Authority Model

a) Testing methodology and findings are owned by the penetration testing team and overseen by the Service Manager.

b) Scope, authorisation, and scheduling are jointly agreed with the Client Test Lead.

c) Operational delivery issues are managed by the Test Lead.

d) Commercial and contractual matters are managed by the Account Manager.

e) Findings and risk ratings are evidence-based and not subject to client approval or modification.

9.9.1 This separation of responsibilities ensures independence, transparency, and defensibility of penetration testing outcomes.

9.10 Service RACI Matrix

9.10.1 The following RACI matrix defines roles and responsibilities for the delivery of the Penetration Testing Service. It clarifies accountability and ownership across key activities to ensure effective governance, communication, and execution throughout the engagement. The matrix identifies who is Responsible, Accountable, Consulted, and Informed for each activity, supporting clear decision-making, efficient escalation, and coordinated incident response.

Activity / Task	*Account Manager*	*Service Manager*	*Test Lead*	*Penetration Tester*	*Client Test Lead*	*Client SMEs*
Engagement initiation & onboarding	R	A	C	I	C	I
Commercial terms & programme setup	A	C	I	I	C	I
Scope definition & authorisation	C	A	R	I	R	C
Scheduling & testing windows	C	A	R	I	R	I
Rules of engagement confirmation	I	A	R	C	C	I
Access & credential coordination	I	C	R	I	R	C
Penetration testing execution	I	C	A	R	I	I
Vulnerability identification & exploitation	I	C	A	R	I	I
Risk assessment & severity rating	I	A	R	C	I	C
Critical finding escalation	I	A	R	C	C	I

Status updates & communications	C	A	R	I	C	I
Report drafting (technical & executive)	I	A	R	C	I	I
Report quality assurance & approval	I	A	C	I	I	I
Close-out & findings walkthrough	C	A	R	I	C	I
Access removal & clean-up confirmation	I	C	R	I	A	I
Retesting (if applicable)	I	A	R	C	C	I
Service closure & offboarding	R	A	C	I	C	I

10. Technical Requirements

10.1.1 Delivery of the Penetration Testing Service requires appropriate technical, procedural, and operational prerequisites to ensure testing is conducted safely, lawfully, and effectively. These requirements are confirmed during onboarding and may be refined as part of detailed scoping.

10.2 Authorisation and Legal Approval

10.2.1 Written authorisation must be provided confirming permission to conduct penetration testing against all in-scope systems, applications, networks, and environments.

10.2.2 Authorisation must clearly define scope boundaries, testing permissions, and any prohibited activities.

10.2.3 The client must confirm legal ownership or authority over all in-scope assets, including third-party or cloud-hosted systems.

10.2.4 Where required, approvals from cloud providers, managed service providers, or third parties must be obtained in advance.

10.2.5 Testing will not commence without confirmed authorisation.

10.3 Defined Scope and Asset Information

10.3.1 A clearly defined scope must be provided, including IP ranges, domains, hostnames, applications, APIs, cloud resources, and environments (e.g. production, staging, development).

10.3.2 The client must identify any business-critical or sensitive systems requiring special handling or restricted testing methods.

10.3.3 Out-of-scope systems must be explicitly identified to prevent unintended impact.

10.3.4 Any changes to scope during testing must be formally agreed and documented.

10.4 Scheduling and Change Management

10.4.1 Testing windows, duration, time-of-day restrictions, blackout periods, and maintenance windows must be agreed during onboarding.

10.4.2 The client must notify relevant internal teams (e.g. SOC, IT operations, service desk) of scheduled testing to avoid misclassification as malicious activity.

10.4.3 Where formal change management or CAB approval is required, this must be completed prior to testing.

10.4.4 Emergency pause or stop-testing procedures must be defined in advance.

10.5 Access and Credentials

10.5.1 Where applicable, valid test credentials (e.g. user accounts, API keys, VPN access) must be provided in advance of testing.

10.5.2 Credentials should be scoped to testing objectives and follow the principle of least privilege unless otherwise agreed.

10.5.3 Any access restrictions, MFA requirements, IP allow-listing, or network segmentation controls must be disclosed.

10.5.4 Delays or limitations in access provision may impact testing timelines and coverage.

10.6 Network and Environment Readiness

10.6.1 Network connectivity must allow testing traffic from agreed source addresses or tester locations.

10.6.2 Firewalls, intrusion prevention systems, and security tooling should be configured to permit authorised testing where appropriate.

10.6.3 The client must advise of any rate-limiting, automated blocking, or defensive controls that may affect testing behaviour.

10.6.4 Testing may be limited where controls cannot be adjusted without unacceptable operational risk.

10.7 Logging, Monitoring and Detection

10.7.1 The client is encouraged to enable appropriate logging and monitoring during testing to support detection and response validation.

10.7.2 Where agreed, testing activities may be used to assess alerting and detection capabilities.

10.7.3 Any requirements for advance notification of specific test phases must be documented.

10.8 Operational Risk and Stability

10.8.1 The client acknowledges that penetration testing involves active exploitation techniques that may expose system weaknesses.

10.8.2 Testing is conducted to minimise disruption; however, residual risk of service impact cannot be entirely eliminated.

10.8.3 Systems known to be unstable, legacy, or unsupported must be identified during scoping.

10.8.4 The client is responsible for ensuring appropriate backups and recovery measures are in place prior to testing.

10.9 Data Protection and Sensitivity

10.9.1 The client must identify systems handling personal, regulated, or highly sensitive data.

10.9.2 Testing approaches may be adjusted to reduce data exposure risk where required.

10.9.3 Any access to sensitive data during testing is limited to what is necessary to demonstrate impact and is handled confidentially.

10.9.4 Data captured as evidence is minimised and protected in line with agreed data handling requirements.

10.10 Secure Communications

10.10.1 Secure communication channels must be used for all exchange of credentials, reports, and sensitive information.

10.10.2 Approved methods for sharing findings, evidence, and reports are agreed during onboarding.

10.10.3 Encryption requirements for report delivery are confirmed in advance.

10.11 Third-Party and Cloud Environments

10.11.1 For cloud or SaaS environments, the client must confirm provider testing policies and constraints.

10.11.2 Some platforms may restrict testing techniques or require provider notification.

10.11.3 Limitations imposed by third parties may reduce testing depth and are documented in reporting.

10.12 Client Resources and Availability

10.12.1 Availability of nominated client contacts is required during testing to support escalation, access issues, or pause requests.

10.12.2 SMEs may be required to validate system behaviour or assist with interpretation of findings.

10.12.3 Delays in client availability may impact delivery timelines.

10.13 Assumptions and Limitations

10.13.1 Penetration testing provides a point-in-time assessment and does not guarantee identification of all vulnerabilities.

10.13.2 Results are dependent on scope definition, access provided, and environmental conditions.

10.13.3 Automated scanning tools may be used to support testing but do not replace manual analysis.

11. Exit and Offboarding

11.1 Service Conclusion

11.1.1 The Penetration Testing Service concludes once all agreed testing activities, validation tasks, and reporting obligations have been completed in accordance with the defined scope and engagement objectives.

11.1.2 Service exit and offboarding are managed in a controlled and documented manner to ensure clarity of outcomes, secure handling of testing artefacts, and appropriate closure of access and credentials.

11.1.3 No further testing or advisory activity (unless retesting) is undertaken beyond service conclusion unless expressly authorised under a new or extended engagement.

11.2 Final Deliverables

11.2.1 At service completion, the agreed deliverables are formally provided to the organisation or its authorised representatives. Deliverables typically include:

a) A technical penetration testing report detailing scope, methodology, findings, severity ratings, exploitation evidence, and remediation guidance

b) An executive summary suitable for senior management and non-technical stakeholders

c) Supporting evidence artefacts, where appropriate and proportionate

d) Retesting results or validation statements, where retesting has been performed

11.2.2 All deliverables are subject to internal quality assurance prior to release to ensure accuracy, consistency, and alignment with recognised testing standards.

11.2.3 Delivery formats, encryption requirements, and secure transfer mechanisms are agreed during onboarding and applied at service completion.

11.3 Knowledge Transfer and Close-out

11.3.1 A close-out meeting is typically conducted to review findings, explain identified risks, and clarify remediation priorities. The close-out session may include:

a) Walkthrough of critical and high-risk findings

b) Explanation of exploitation paths and impact

c) Clarification of assumptions, limitations, and scope boundaries

d) Discussion of remediation approaches and security improvement opportunities

11.3.2 Knowledge transfer is tailored to relevant stakeholders, including security teams, IT operations, risk management, and senior leadership, as appropriate.

11.4 Access, Credentials, and System Clean-up

11.4.1 All test accounts, credentials, VPN access, or temporary permissions provided for testing are securely deleted, revoked, or returned following completion of testing.

11.4.2 Any configuration changes made solely to enable testing are reversed unless otherwise agreed.

11.4.3 Confirmation of access removal may be provided to the client upon request.

11.5 Data Handling and Retention

11.5.1 All testing data, evidence artefacts, notes, and reports are handled in accordance with agreed confidentiality, data protection, and retention requirements.

11.5.2 Data is stored securely during the engagement in access-controlled environments appropriate to its sensitivity.

11.5.3 Following service completion, data is either:

a) Securely transferred to the client, and/or

b) Retained for an agreed period to support remediation, assurance, or regulatory needs

11.5.4 At the end of the agreed retention period, all retained data is securely destroyed in line with documented procedures unless alternative instructions are received in writing.

11.6 Acceptance of Deliverables

11.6.1 Deliverables are deemed accepted once issued and no material issues are raised within an agreed review period.

11.6.2 Requests for factual clarification or minor amendments may be addressed as part of close-out. Requests for additional testing or expanded analysis require a separate engagement.

11.7 Service Closure

11.7.1 The service is formally closed once:

a) All agreed deliverables have been provided

b) Access and credentials have been revoked

c) Data handling and retention arrangements are confirmed

11.7.2 Any further support beyond service closure, including additional testing, remediation validation, or programme-based testing, is subject to a new or extended agreement.

*****END OF DOCUMENT*****