Post Breach Incident Review Service Definition

Document title	Post Breach Incident Review Service Definition		
Reference No.	IF-SER-027	**Version**	1.0
Author	Holly Jackson, Cyber Manager		
Reviewed by	Lisa Washer, Head of Cyber		
Issue date	26/01/2026		

Post Breach Incident Review Service Definition

Document Control

Version	Name	Comment	Date
0.1	Holly Jackson	Initial Draft	07/01/2026
0.2	Lisa Washer	Review and amendments	25/01/2026
1.0	Holly Jackson	Final review and publish	26/01/2026

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

Post Breach Incident Review Service Definition

Contents

1. Post Breach Incident Review Service

1.1 Service Overview

1.1.1 The Post Breach Incident Review Service provides an independent, structured assessment following a cyber security incident or data breach. The service is designed to evaluate the causes, handling, and impact of the incident, and to identify lessons learned and corrective actions to strengthen the organisation's security posture, governance, and regulatory compliance.

1.1.2 The service supports organisations that have experienced a confirmed or suspected breach and require assurance over the effectiveness of their incident response, containment actions, decision-making, and technical controls. It is particularly suited to organisations operating in regulated environments, including those subject to data protection, financial services, or critical infrastructure obligations.

2. Service Features

2.1.1 A structured, impartial review conducted by experienced cyber and forensic specialists, independent of the original incident response team, to provide objective findings and assurance.

2.2 Incident Timeline and Root Cause Analysis

2.2.1 Reconstruction of the incident timeline using available evidence to identify:

a) Initial point of compromise

b) Attack progression and dwell time

c) Control failures and contributing factors

d) Root technical and procedural causes

2.3 Assessment of Incident Response Effectiveness

2.3.1 Evaluation of the organisation's response against internal procedures and recognised good practice, including:

a) Detection and escalation

b) Containment and eradication

c) Decision-making and communications

d) Use of third parties and escalation paths

2.4 Control and Compliance Review

2.4.1 Assessment of relevant security controls and practices in place at the time of the incident, with consideration of:

a) Applicable regulatory or contractual requirements (e.g. PCI DSS)

b) Policy adherence

c) Control design versus operational effectiveness

2.5 Actionable Improvement Recommendations

2.5.1 Clear, prioritised recommendations focused on preventing recurrence, improving resilience, and strengthening governance, supported by pragmatic remediation guidance.

3. Service Benefits

3.1.1 Below is a list of the key outcomes and advantages the customer gains from using the service.

a) **Provides independent assurance over the handling and impact of a cyber incident -** Offers an objective assessment of incident management, containment actions, and outcomes, supporting confidence in findings and conclusions.

b) **Enables organisations to clearly understand what happened and why -** Presents a clear, evidence-led account of the incident, including key events, attack methods, and underlying causes.

c) **Identifies gaps in technical controls, processes, and decision-making -** Highlights weaknesses across technology, governance, and response activities that contributed to the incident.

d) **Supports regulatory, audit, and board-level reporting requirements -** Produces structured findings suitable for regulatory engagement, audit review, and senior management reporting.

e) **Helps prevent repeat incidents through targeted, evidence-based improvements -** Provides focused recommendations addressing root causes to reduce the likelihood of recurrence.

f) **Strengthens organisational cyber maturity and incident preparedness -** Informs improvements to controls, governance, and response capability to enhance future resilience.

4. Scope of Service

4.1 In-scope Activities

4.1.1 The following activities are within the scope of the service:

a) Review of incident documentation, logs, alerts, and available evidence

b) Stakeholder interviews with relevant technical, security, and management staff

c) Reconstruction of the incident timeline and key decisions

d) Assessment of incident response processes and execution

e) Review of relevant technical and organisational security controls

f) Identification of root causes and contributing factors

g) Production of a formal written review report with findings and recommendations

4.2 Out-of-scope Activities

4.2.1 The following activities are outside of the scope of this service:

a) Live incident response or containment activities

b) Full digital forensic acquisition and analysis unless explicitly agreed

c) Legal, regulatory, or public relations advice

d) Implementation of remediation actions

e) Penetration testing or vulnerability scanning outside the incident scope

4.3 Assumptions and Dependencies

4.3.1 The following list outlines the assumptions and dependencies for the service to produce the required outcome:

a) Timely access to relevant systems, logs, and documentation

b) Availability of key personnel for interviews and clarification

c) Accuracy and completeness of information provided by the customer

d) Cooperation from third parties where evidence is externally held

5. Onboarding

5.1.1 Onboarding begins once contractual agreement has been completed and the scope of the service has been formally confirmed. This stage establishes the foundation for effective delivery and ensures clarity of roles, expectations, and timelines from the outset.

5.1.2 As part of onboarding, customer and service delivery points of contact are appointed to enable clear communication and accountability. An initial scoping call is conducted to confirm service objectives, delivery timeframes, and any constraints or dependencies affecting the review. Secure access arrangements are then agreed to enable the safe exchange of documentation and evidence relevant to the incident, alongside agreement on communication cadence and escalation routes throughout the engagement.

5.1.3 The onboarding process ensures the post-breach review can proceed efficiently, consistently, and in line with agreed scope and expectations.

6. Service Delivery Model

6.1 Engagement Approach

6.1.1 Service delivery is primarily conducted remotely, leveraging secure communication and collaboration channels to enable timely and efficient engagement. Where appropriate, delivery may be provided through a hybrid model or on-site presence, subject to customer requirements, sensitivity of the incident, or practical considerations.

6.2 Delivery Phases

6.2.1 The service is delivered through a structured and repeatable review methodology designed to ensure consistency, quality, and defensibility of findings. The methodology is proportionate to the nature of the incident and is adapted based on scale, complexity, and risk. The key phases of delivery are outlined below.

a) **Initiation and scoping** - This phase establishes the objectives, scope, and boundaries of the review. It includes confirmation of in-scope systems and timeframes, identification of key stakeholders, validation of assumptions, and agreement of delivery timelines, communication cadence, and escalation routes.

b) **Evidence gathering and review** - Relevant documentation, logs, alerts, and other available artefacts are collected and reviewed in a secure manner. This may include incident records, security tooling outputs, policies and procedures, and third-party information where applicable. Stakeholder interviews are conducted to assist in understanding actions taken, decisions made, and contextual factors.

c) **Analysis and assessment** - Collected evidence is analysed to reconstruct the incident timeline and assess the effectiveness of technical controls, processes, and decision-making. This phase focuses on identifying root causes, contributing factors, and control failures, rather than symptoms alone, using an evidence-based approach.

d) **Findings development** - Clear, structured findings are developed based on the analysis, supported by factual evidence. Findings include identification of weaknesses, impact assessment, and contributing organisational or technical issues, along with prioritised improvement areas.

e) **Reporting and close-out** - A formal review report is produced, summarising the incident, key findings, and recommended actions. The report is shared with relevant stakeholders, feedback is incorporated where appropriate, and the engagement is formally closed, with evidence handled in line with agreed data management requirements.

7. Support Model

7.1.1 Standard support is provided during normal business hours, with clearly defined points of contact responsible for service delivery, coordination, and escalation. These points of contact ensure consistent communication, timely issue resolution, and effective management of customer queries throughout the engagement.

7.1.2 Escalation routes are established during onboarding to ensure that risks, constraints, or delivery issues are addressed promptly and at the appropriate level. Where required, enhanced or expedited support may be made available by prior agreement, subject to resource availability and contractual terms. This may include extended support hours, accelerated timelines, or additional specialist involvement to address incident severity or business criticality.

8. Service Level Agreements

8.1.1 The following service levels describe indicative performance targets for the service. These service levels are provided for guidance only and do not constitute guaranteed commitments unless expressly agreed in writing.

8.2 Response time

8.2.1 Initial engagement typically commences within 3–5 business days of receipt of formal instruction and contractual confirmation. This timeframe is subject to resource availability and the readiness of required information, including access to relevant documentation, systems, and key stakeholders. Where dependencies are met promptly, the service will mobilise without unnecessary delay to ensure timely commencement of the review.

8.3 Delivery timeframe

8.3.1 Typical review delivery ranges from 2 to 6 weeks from commencement, depending on the complexity and scale of the incident, the volume and quality of available evidence, and the availability of key stakeholders for interviews and clarification. Timelines may also be influenced by third-party dependencies, the age of the incident, and the level of technical analysis required. Where constraints are identified, delivery timeframes are discussed and agreed early in the engagement to ensure expectations are managed appropriately.

8.4 Reporting turnaround

8.4.1 Reports are typically provided within 10 business days following the completion of evidence collection and analysis. This timeframe allows for the consolidation of findings, quality assurance review, and preparation of a structured report that clearly documents the incident overview, key findings, and recommendations.

9. Technical Requirements

9.1.1 Delivery of the service requires appropriate technical access, information, and resources to enable effective activities. The following requirements apply and are confirmed during onboarding.

a) **Secure method for document and evidence sharing** - Access to a secure mechanism for the transfer and storage of documentation and evidentiary materials, such as incident records, logs, and supporting artefacts must be provided.

b) **Access to relevant security tooling outputs and logs (where available)** - Access is required to outputs from relevant security tools and platforms, including log data, alerts, dashboards, and incident records, where available. This information supports accurate reconstruction of events, validation of detection and response activities, and assessment of control effectiveness during the incident period.

c) **Read-only access where system access is required**- Where system access is necessary to support the review, access will be limited to read-only permissions to prevent any impact on live environments. Access is granted solely for the purpose of evidence review and analysis and is restricted to systems and timeframes within the agreed scope.

d) **Ability to conduct remote interviews using approved communication platforms** - The customer must be able to participate in remote interviews using approved and secure communication platforms. These interviews support clarification of evidence, understanding of actions taken, and validation of incident handling, and are scheduled in line with stakeholder availability and agreed delivery timelines.

10. Exit and Offboarding

10.1.1 Service exit occurs upon formal delivery of the final report and any agreed supporting materials. At this point, the post-breach incident review engagement is considered complete, subject to any agreed follow-up activities.

10.1.2 Confirmation of service completion is provided to the customer, ensuring clear closure of the engagement. Where required, optional knowledge transfer or a follow-up briefing may be delivered to support understanding of the findings, recommendations, and next steps.

11. Roles and Responsibilities

11.1.1 The following are the main roles and responsibilities expected of staff.

11.2 Service Provider

11.2.1 The Service Provider is responsible for delivering the post-breach incident review in line with the agreed scope, objectives, and methodology. This includes conducting the review with due professional care, maintaining the confidentiality of all customer information, and ensuring the integrity and appropriate handling of all evidence throughout the engagement. The Service Provider will produce clear, accurate, and well-supported findings and recommendations, based on evidence gathered and analysed during the review.

11.3 Customer

11.3.1 The Customer is responsible for providing timely access to relevant information, systems, and personnel required to support the review. This includes nominating a single point of contact to coordinate activities, facilitate communication, and manage internal dependencies. The Customer is also responsible for validating the factual accuracy of findings shared during the engagement to ensure reports accurately reflect the incident and associated context.

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