Incident Response Planning & Testing Service Definition

Document title	Incident Response Planning & Testing Service Definition		
Reference No.	IF-ser-024	**Version**	1.0
Author	Holly Jackson, Cyber Manager		
Reviewed by	Lisa Washer, Head of Cyber		
Issue date	23/01/2026		

Incident Response Planning & Testing Service Definition

Document Control

Version	Name	Comment	Date
0.1	Holly Jackson	Initial draft	07/01/2026
0.2	Lisa Washer	Review and amendments	23/01/2026
1.0	Holly Jackson	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

Incident Response Planning & Testing Service Definition

Contents

1. Incident Response Planning & Testing Service

1.1 Service Overview

1.1.1 The Incident Response Planning and Testing Service supports organisations in developing, validating, and assessing their cyber incident response capability. The service includes the creation of a tailored Incident Response (IR) Plan, followed by structured assessment and testing to evaluate its effectiveness, practicality, and alignment with organisational needs and regulatory expectations.

1.1.2 The service is designed for organisations seeking to improve preparedness for cyber incidents, reduce response times, and ensure roles, responsibilities, and escalation processes are clearly defined and understood. It is suitable for both organisations establishing an incident response capability for the first time and those seeking independent assurance over existing plans.

1.1.3 Outputs are evidence-based and practical, enabling organisations to demonstrate preparedness while identifying areas for improvement before an incident occurs.

2. Service Features

2.1.1 Below are a list of the core capabilities and characteristics of the service.

- **Incident Response Plan Development** - Development of a tailored Incident Response Plan aligned to the organisation's size, risk profile, operating environment, and regulatory obligations. The plan defines roles, responsibilities, escalation paths, decision-making authority, and response procedures across the incident lifecycle.
- **Alignment to Standards and Good Practice** - The IR Plan and assessment approach are informed by recognised frameworks and standards, such as ISO/IEC 27001, regulatory guidance, and industry good practice, ensuring suitability for audit, assurance, and regulatory review.
- **Incident Response Plan Review and Assessment** - Independent assessment of the Incident Response Plan to evaluate completeness, clarity, and effectiveness. This includes review of governance, technical response steps, communications, and dependency management.
- **Tabletop Exercise and Scenario-Based Testing** - Facilitated tabletop exercises or scenario-based testing to assess plan effectiveness in practice. Exercises test decision-making, escalation, communications, and coordination under realistic incident conditions.
- **Findings and Improvement Recommendations** - Clear, prioritised findings and recommendations focused on strengthening incident response capability, closing gaps, and improving operational readiness.

3. Service Benefits

3.1.1 A list of the key outcomes and advantages the customer gains from using the service are outlined below.

- **Establishes a clear, structured, and fit-for-purpose Incident Response Plan** - Provides a documented, organisation-specific Incident Response Plan that defines how cyber incidents are identified, managed, and resolved.
- **Improves organisational readiness to respond effectively to cyber incidents** - Enhances preparedness by ensuring processes, decision-making frameworks, and response procedures are defined and understood in advance, reducing reliance on ad-hoc responses during high-pressure incident scenarios.
- **Clarifies roles, responsibilities, and escalation paths before an incident occurs** - Clearly defines accountability, authority, and communication routes across technical, management, and executive stakeholders, helping to ensure timely escalation and coordinated response when an incident occurs.
- **Identifies gaps in planning, governance, and response capability** - Highlights deficiencies in documentation, control coverage, decision-making, and coordination through structured review and testing, enabling organisations to address weaknesses proactively.
- **Supports audit, regulatory, and assurance requirements** - Produces documented evidence of incident response planning and testing that can be used to demonstrate compliance, due diligence, and preparedness to auditors, regulators, and other assurance bodies.
- **Reduces response time, confusion, and impact during real incidents** - By testing and validating response arrangements in advance, the service helps minimise uncertainty, delays, and operational disruption during actual cyber incidents, reducing overall impact to the business.

4. Scope of Service

4.1.1 The following defines what is included and excluded within the service.

4.2 In-scope Activities

- Development or refinement of an Incident Response Plan
- Review of existing policies, procedures, and supporting documentation
- Stakeholder workshops and interviews
- Scenario design and tabletop exercise facilitation
- Assessment of plan effectiveness and response readiness
- Production of formal findings and recommendations

4.3 4.2 Out-of-scope Activities

- Live incident response or containment activities
- Technical penetration testing or red-team exercises
- Implementation of recommended improvements
- Legal, regulatory, or public relations advisory services

4.4 4.3 Assumptions and Dependencies

- Availability of relevant stakeholders for workshops and exercises
- Access to existing documentation and organisational context
- Timely customer feedback and clarification

5. Onboarding

5.1.1 Onboarding begins following contractual agreement and confirmation of scope. The onboarding process includes appointment of customer and service delivery points of contact, an initial scoping discussion to confirm objectives and timelines, and agreement of access requirements and communication cadence. Onboarding ensures the service can be delivered efficiently and in line with agreed expectations.

6. Service Delivery Model

6.1.1 The service is delivered through a structured, staged approach designed to ensure consistency, quality, and practical relevance.

6.2 Delivery Phases

6.2.1 Delivery typically comprises three core phases:

- **Incident Response Plan development** - focused on creating a documented, organisation-specific response framework.
- **Incident Response Plan review** - assessing completeness, clarity, and alignment with organisational requirements and good practice.
- **Structured testing** - using scenario-based or tabletop exercises to evaluate the practical effectiveness of the plan.

6.2.2 Each phase builds on the outcomes of the previous phase, ensuring that final deliverables are fully informed by organisational context, validated through review, and supported by evidence-based testing.

6.3 Engagement Approach & Modes

6.3.1 Delivery is typically conducted remotely using secure collaboration and communication platforms, enabling efficient engagement with stakeholders across the organisation. Where required, a hybrid or on-site delivery model can be accommodated to support workshops, tabletop exercises, or stakeholder sessions, subject to customer requirements and practical considerations.

6.3.2 The delivery approach is tailored to the organisation's cyber maturity, operating complexity, and risk profile. This ensures that the depth of content, level of challenge, and testing scenarios are proportionate to the organisation's size, regulatory obligations, and threat landscape. The service is designed to be pragmatic and scalable, focusing on producing usable, actionable outcomes rather than generic documentation.

7. Support Model

7.1.1 Standard support is provided during normal business hours, with clearly defined delivery and escalation points of contact established at the outset of the engagement. These contacts are responsible for coordinating service activities, managing communications, and addressing queries or issues that arise during delivery, ensuring continuity and effective oversight throughout the service lifecycle.

7.1.2 Escalation paths are agreed during onboarding to ensure that risks, dependencies, or delivery challenges are addressed promptly and at the appropriate level. Where additional support is required, enhanced service options may be made available by prior agreement. These may include extended support hours, additional planning or testing workshops, or expedited delivery timelines, subject to resource availability and the terms of the applicable contract.

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 response timeframe is dependent on resource availability and the readiness of required information, including access to relevant documentation, systems, and nominated points of contact. Where dependencies are met promptly, mobilisation will occur without unnecessary delay.

8.3 Delivery timeframe

8.3.1 Typical delivery ranges from 4 to 8 weeks from commencement. Delivery timelines are influenced by factors such as the organisation's size and complexity, the number and availability of stakeholders required to participate, and the depth of incident response planning, review, and testing activities included in scope. Any anticipated impacts to delivery timeframes are identified and discussed early to ensure expectations are managed effectively.

8.4 Reporting turnaround

8.4.1 Reporting outputs are typically provided within 10 business days of completing review and testing activities. This timeframe allows for consolidation of findings, internal quality assurance, and preparation of final deliverables that accurately reflect the scope of work undertaken.

9. Technical Requirements

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

- **Secure method for document sharing -** Provide access to a secure mechanism for the exchange of documents and artefacts relevant to the service. This includes policies, plans, and supporting materials.
- **Access to relevant policies and supporting documentation -** Access is required to current and relevant organisational policies, procedures, and supporting documentation, including existing incident response, information security, and governance materials.
- **Availability of key stakeholders for workshops and exercises -** Key stakeholders must be available to participate in workshops, interviews, and scenario-based testing sessions. This includes representatives from technical, security, operational, and management functions, whose input is necessary to validate roles, responsibilities, decision-making, and escalation during incident response activities.
- **Ability to conduct remote sessions using approved communication platforms -** The customer must be able to support the delivery of remote workshops, interviews, and exercises using approved and secure communication platforms.

10. Exit and Offboarding

10.1.1 Service exit occurs upon the delivery of all final documentation and formal confirmation that the service has been completed in line with the agreed scope and objectives. At this point, the engagement is considered closed, subject to any separately agreed follow-up activities.

10.1.2 Offboarding activities include the secure handling of all customer data, materials, and artefacts generated or obtained during delivery. Where appropriate, optional follow-up briefings or knowledge-transfer sessions may be provided to support customer understanding of findings, recommendations, and next steps, ensuring outputs are clearly understood and can be effectively actioned.

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 Incident Response Planning and Testing service in accordance with the agreed scope, objectives, and delivery methodology. This includes designing, developing, and documenting an organisation-specific Incident Response Plan, as well as planning and facilitating structured reviews and scenario-based testing activities. The Service Provider will apply recognised incident response good practice and industry standards to ensure the plan is practical, proportionate, and aligned to the organisation's risk profile and operating environment.

11.2.2 The Service Provider is also responsible for assessing the effectiveness of the Incident Response Plan through testing, identifying gaps in preparedness, governance, and execution. Clear, accurate, and evidence-based outputs will be produced, including documented findings and recommendations, to support informed decision-making and improvements to incident response capability.

11.3 Customer

11.3.1 The Customer is responsible for providing timely access to relevant information, policies, and supporting documentation required to develop and assess the Incident Response Plan. This includes making available key personnel from technical, security, operational, and management functions to participate in workshops, interviews, and testing exercises.

11.3.2 The Customer is also responsible for nominating a single point of contact to coordinate service activities, facilitate communication, and manage internal dependencies. The Customer will support the validation of factual accuracy within deliverables to ensure that outputs accurately reflect organisational context, roles, and response arrangements.

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