

MSP SERVICE DELIVERY ASSESSMENT

A practical assessment for evaluating how managed security services operate beyond monitoring.

Choosing a managed security service is not only about comparing technologies or monitoring capabilities.

Many providers offer similar detection tools and dashboards. The differences become visible when incidents require investigation, decision-making, response, communication, and follow-up.

This assessment helps evaluate the operational maturity of a managed security service.

It can be used to assess an existing service, support internal discussions, or compare potential managed security providers.

HOW TO USE THIS ASSESSMENT

Review each statement and select the answer that best reflects how the process works in practice.

Yes

The process is clearly defined, documented, and implemented consistently.

Partially

The process exists, but it is not fully documented, standardized, or applied consistently.

No

The process is not formally defined or is not currently implemented.

The objective is not simply to achieve the highest possible score. Use the results to identify unclear responsibilities, inconsistent processes, and areas where service delivery can be strengthened.

SCORING

Assign:

- 2 points for every Yes
- 1 point for every Partially
- 0 points for every No

Maximum score: 40 points

MSP SERVICE DELIVERY ASSESSMENT

A practical assessment for evaluating how managed security services operate beyond monitoring.

1. MONITORING

Monitoring creates visibility across the protected environment. Its value depends on clearly defined coverage, relevant data sources, and consistent prioritization.

Assessment statement	Yes	Partially	No
Security events are monitored continuously.	☐	☐	☐
The systems, endpoints, identities, applications, and network sources included in the service are clearly	☐	☐	☐
Monitoring coverage and exclusions are documented.	☐	☐	☐
Alerts are prioritized according to consistent severity and business-impact criteria.	☐	☐	☐

Section score: ____ / 8

Notes:

2. INVESTIGATION

Investigation transforms an alert into an informed assessment. It adds technical and business context before escalation or response.

Assessment statement	Yes	Partially	No
Alerts are validated before they are escalated as security incidents.	☐	☐	☐
Investigations consider the affected asset, identity, business service, and potential operational impact.	☐	☐	☐
False positives and recurring benign events are documented and reviewed.	☐	☐	☐
Analysts follow standardized investigation procedures or playbooks.	☐	☐	☐

Section score: ____ / 8

Notes:

MSP SERVICE DELIVERY ASSESSMENT

A practical assessment for evaluating how managed security services operate beyond monitoring.

3. RESPONSE

Response turns security analysis into coordinated action. Effective response depends on clear authority, assigned responsibilities, and predefined procedures.

Assessment statement	Yes	Partially	No
Response actions and escalation paths are documented.	☐	☐	☐
Responsibilities between the provider, the client, and any third parties are clearly assigned.	☐	☐	☐
Containment procedures are defined for common incident scenarios.	☐	☐	☐
Authorized response decisions can be approved and executed without unnecessary delay.	☐	☐	☐

Section score: ____ / 8

Notes:

4. COMMUNICATION

Communication keeps technical teams, management, and other stakeholders aligned throughout an incident.

Assessment statement	Yes	Partially	No
The client receives timely updates during active incidents.	☐	☐	☐
Responsibilities for technical, management, and regulatory communication are clearly assigned.	☐	☐	☐
Technical findings and executive updates are adapted to their intended audiences.	☐	☐	☐
Incident timelines, actions, decisions, and current status are communicated clearly.	☐	☐	☐

Section score: ____ / 8

Notes:

MSP SERVICE DELIVERY ASSESSMENT

A practical assessment for evaluating how managed security services operate beyond monitoring.

5. CONTINUOUS IMPROVEMENT

A mature service does not end when the incident is closed. It uses operational experience to improve detection, response, and future service delivery.

Assessment statement	Yes	Partially	No
Significant incidents are reviewed after closure.	☐	☐	☐
Lessons learned and improvement actions are documented.	☐	☐	☐
Detection rules, response procedures, and playbooks are updated when needed.	☐	☐	☐
Recurring incidents, operational bottlenecks, and service trends are tracked over time.	☐	☐	☐

Section score: ____ / 8

Notes:

SCORING

- 2 points for every Yes
- 1 point for every Partially
- 0 points for every No

Area	Score
Monitoring	____ / 8
Investigation	____ / 8
Response	____ / 8
Communication	____ / 8
Continuous Improvement	____ / 8
Total	____ / 40

MSP SERVICE DELIVERY ASSESSMENT

A practical assessment for evaluating how managed security services operate beyond monitoring.

UNDERSTANDING YOUR RESULT

32–40 points

Operationally Mature

The service demonstrates a structured and well-defined delivery model.

Core processes are documented and applied consistently across monitoring, investigation, response, communication, and continuous improvement.

Review individual “Partially” or “No” answers to identify targeted opportunities for refinement.

22–31 points

Operationally Developing

The main operational processes are in place, but some areas may depend on informal practices, individual knowledge, or inconsistent execution.

Prioritize the sections with the lowest scores and clarify responsibilities, escalation paths, response authority, and documentation.

0–21 points

Operational Gaps Identified

Monitoring capabilities may be available, but important elements of service delivery remain undefined, undocumented, or inconsistently implemented.

Focus first on the areas that affect incident response directly: ownership, escalation, response authority, communication, and repeatable procedures.

REVIEW THE RESULTS BY SECTION

The total score provides an overall view, but the individual section scores are equally important.

A high monitoring score does not compensate for unclear response authority.

Strong investigation capabilities do not guarantee effective service delivery when communication or escalation processes are inconsistent.

MSP SERVICE DELIVERY ASSESSMENT

A practical assessment for evaluating how managed security services operate beyond monitoring.

USE THE SECTION RESULTS TO ANSWER THREE PRACTICAL QUESTIONS:

Where are the most significant operational gaps?

Identify the areas with the lowest scores or the highest number of “No” responses.

Which gaps could delay action during an incident?

Prioritize unclear responsibilities, approval requirements, escalation paths, and containment authority.

Which improvements can be implemented first?

Select a small number of actions that can be assigned, documented, and reviewed within a defined period.

Priority area	Required action	Owner	Target date
1			
2			
3			

WHAT DOES THIS ASSESSMENT TELL YOU?

A high score does not guarantee that incidents will never occur.

A lower score does not necessarily indicate weak technology.

The assessment shows how consistently the managed security service is delivered when an event requires investigation, decisions, response, communication, and follow-up.

Technology creates visibility.

Operational processes turn that visibility into a reliable managed service.

MSP SERVICE DELIVERY ASSESSMENT

A practical assessment for evaluating how managed security services operate beyond monitoring.

NEXT STEP

Use the completed assessment as a discussion framework with your internal team or managed security provider.

Review unclear answers, assign responsibility for priority improvements, and repeat the assessment periodically to track progress.

Need support evaluating or strengthening your managed security operating model?

DIAMATIX combines technology, defined operational processes, and 24/7 security expertise to help organizations build a more consistent and resilient approach to detection and response.

[DISCUSS YOUR OPERATING MODEL](#)

MSP SERVICE DELIVERY ASSESSMENT

A practical assessment for evaluating how managed security services operate beyond monitoring.

© DIAMATIX 2026. All rights reserved.

This material is provided for informational and educational purposes only and reflects operational observations at the time of publication.

While every effort has been made to ensure accuracy, security practices, regulatory requirements, and operational conditions may change over time.

This document does not constitute legal, regulatory, or technical advice.

DIAMATIX is not responsible for decisions made based solely on this material without additional professional consultation.

For up-to-date guidance or a tailored discussion, contact:

+359 876 328030

info@diamatix.com

www.diamatix.com

Trusted · Innovative · Vigilant