NIST CSF Questionnaire (Detect, Respond, Recover)

As part of our annual Risk Assessment, we need input for the information in this form.

* This form will record your name, please fill your name.

DETECT Continuous Monitoring - DE.CM-01

Networks and network services are monitored to find potentially adverse events

1. Is there a formal policy that specifies how network monitoring is conducted, what metrics are important, and how alerts should be handled?

   ○ Yes

   ○ No

   ○ N/A

   ○ Other

2. Are there logs from an IDS that show detected suspicious activities, including timestamps, the nature of the activity, and the network segments affected?

   ○ Yes

   ○ No

   ○ N/A

   ○ Other

3. Are there logs or reports showing updates to monitoring tools or adjustments to configurations in response to new security threats or after an incident

○ Yes

○ No

○ N/A

○ Other

4. Are there certificates or records of training sessions attended by network security personnel, showing dates and the content of the training?

○ Yes

○ No

○ N/A

○ Other

DETECT Continuous Monitoring - DE.CM-02

The physical environment is monitored to find potentially adverse events

5. Is there a comprehensive document that details all physical security controls, monitoring practices, and response procedures?

○ Yes

○ No

○ N/A

○ Other

6. Are there records from an access control system showing entry and exit logs, including date, time, and badge details of personnel accessing secure areas?

○ Yes

○ No

○ N/A

○ Other

7. Are there summaries or clips from CCTV footage capturing specific events of interest, such as unauthorized access attempts or detection of environmental hazards?

○ Yes

○ No

○ N/A

○ Other

8. Are there records of alerts from environmental sensors, such as high temperature, smoke detection, or water leakage, including the time of the alert and the response initiated?

○ Yes

○ No

○ N/A

○ Other

9. Is there a summary from the latest security audit reviewing the physical security measures, highlighting any incidents, breaches, and the efficacy of the surveillance and monitoring systems?

○ Yes

○ No

○ N/A

○ Other

DETECT Continuous Monitoring - DE.CM-06

External service provider activities and services are monitored to find potentially adverse events

10. Is there a policy that outlines the procedures for monitoring external vendors, detailing what aspects of their service are monitored and how data security is ensured?

○ Yes

○ No

○ N/A

○ Other

11. Are there sections of service level agreements that specify the security and monitoring expectations, including performance benchmarks and penalties for non-compliance?

○ Yes

○ No

○ N/A

○ Other

12. Is there a monthly report received from a cloud service provider that includes logs of all access to the organization’s data and any security incidents reported during the period?

○ Yes

○ No

○ N/A

○ Other

13. Is there a summary report from an independent audit performed on a service provider, assessing their compliance with security practices and highlighting any issues found?

○ Yes

○ No

○ N/A

○ Other

14. Is there a detailed report documenting an incident caused by an external service provider, such as unauthorized access or data leakage, including steps taken by both the provider and the organization to address the incident?

○ Yes

○ No

○ N/A

○ Other

RESPOND Incident Management - RS.MA-01

The incident response plan is executed in coordination with relevant third parties once an incident is declared

15. Is there a section of the incident response plan specifically detailing procedures for involving third parties, including contact lists for key external contacts?

○ Yes

○ No

○ N/A

○ Other

16. Are there copies of SLAs with third-party service providers, such as cybersecurity firms or cloud service providers, that include terms related to incident response?

○ Yes

○ No

○ N/A

○ Other

17. Are there any records from joint incident response drills conducted with third parties, showing the date, participants, and outcomes of the drills?

○ Yes

○ No

○ N/A

○ Other

18. Are there Logs showing the timeline of communications with third parties during an incident, detailing who was contacted, when, and what information was exchanged?

○ Yes

○ No

○ N/A

○ Other

19. Is there a report from an after-action review meeting following an incident, evaluating the coordination with third parties and suggesting improvements for future responses?

○ Yes

○ No

○ N/A

○ Other

RESPOND Incident Management - RS.MA-02

Incident reports are triaged and validated

20. Is there a document that outlines how incident reports are processed, including the specific criteria used to assess the severity and authenticity of incident?

○ Yes

○ No

○ N/A

○ Other

21. Are there certificates or records showing that the incident response team has been trained on the latest triage and validation procedure?

○ Yes

○ No

○ N/A

○ Other

22. Is there an example of an incident log entry showing the initial report, the triage decision, steps taken to validate the incident, and the final determination?

○ Yes

○ No

○ N/A

○ Other

23. Is there a summary from an internal audit reviewing the triage and validation processes, highlighting any issues found and recommendations for improvements?

○ Yes

○ No

○ N/A

○ Other

24. Is there a report detailing the findings from a recent quality assurance review of the incident triage and validation process, including any discrepancies noted and corrective actions taken?

○ Yes

○ No

○ N/A

○ Other

RESPOND Incident Management - RS.MA-03

Incidents are categorized and prioritized

25. Is there a document that outlines the criteria for placing incidents into specific categories and the rationale for their priority levels?

○ Yes

○ No

○ N/A

○ Other

26. Are there certificates or records indicating that relevant staff have completed training on the incident categorization and prioritization process?

○ Yes

○ No

○ N/A

○ Other

27. Are there entries from an incident log showing the categorization and prioritization of different incidents, including the rationale for these decisions?

○ Yes

○ No

○ N/A

○ Other

28. Is there a summary from an internal audit that reviews how well incidents are categorized and prioritized, including any findings and recommendations for improvement?

○ Yes

○ No

○ N/A

○ Other

29. Are there documents that record changes to the categorization and prioritization guidelines, including the reasons for these changes and the stakeholders involved?

○ Yes

○ No

○ N/A

○ Other

RESPOND Incident Management - RS.MA-04

Incidents are escalated or elevated as needed

30. Is there a document that defines the escalation process, including the criteria for escalating incidents and the chain of command for elevated incident management?

○ Yes

○ No

○ N/A

○ Other

31. Are there summaries or records from training sessions on incident escalation, indicating the dates these sessions were held and who attended?

○ Yes

○ No

○ N/A

○ Other

32. Is there an example of an incident report that includes an escalation log, showing how the incident was escalated, the justification for escalation, and the outcome?

○ Yes

○ No

○ N/A

○ Other

33. Is there a summary from an internal audit that evaluates the effectiveness of the incident escalation practices, highlighting any issues found and recommendations for improvement?

○ Yes

○ No

○ N/A

○ Other

34. Are there minutes from a meeting where the incident escalation policy was reviewed and updated, including details on what was changed and why?

○ Yes

○ No

○ N/A

○ Other

RESPOND Incident Management - RS.MA-05

The criteria for initiating incident recovery are applied

35. Is there a policy document detailing the specific conditions under which recovery should be initiated, including thresholds for system functionality, security verification, and risk assessment outcomes?

○ Yes

○ No

○ N/A

○ Other

36. Are there records from training sessions focused on the recovery process, including who attended and when, ensuring that all relevant staff are knowledgeable about the criteria?

○ Yes

○ No

○ N/A

○ Other

37. Is there an entry from an incident log that shows the assessment against the recovery criteria and the decision to initiate recovery, including details of the incident severity, impact assessment, and readiness for recovery?

○ Yes

○ No

○ N/A

○ Other

38. Is there a summary from an internal audit reviewing how recovery initiation criteria are applied, noting any discrepancies and suggesting improvements?

○ Yes

○ No

○ N/A

○ Other

RESPOND Incident Management - RS.AN-03

Analysis is performed to establish what has taken place during an incident and the root cause of the incident

39. Is there a document that specifies the approach and techniques used for incident analysis, ensuring a systematic and thorough investigation?

○ Yes

○ No

○ N/A

○ Other

40. Are there certificates or records indicating that analysts have completed specific training in forensic analysis and root cause determination?

○ Yes

○ No

○ N/A

○ Other

41. Is there an example of an incident report that includes a detailed analysis section, showing the incident timeline, the investigative methods used, and the conclusions about the root cause?

○ Yes

○ No

○ N/A

○ Other

42. Are there logs or documentation showing how forensic tools were used in a specific incident analysis, including outputs and results that helped identify the root cause?

○ Yes

○ No

○ N/A

○ Other

43. Is there a summary from a post-incident review meeting, discussing the findings from the incident analysis and recommendations for preventing future incidents based on the root cause analysis?

○ Yes

○ No

○ N/A

○ Other

RESPOND Incident Management - RS.AN-06

Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved

44. Is there a policy document that outlines how to document investigation activities and the methods used to secure these documents?

○ Yes

○ No

○ N/A

○ Other

45. Are there records showing how the integrity of investigation records is checked and verified, including the tools and processes used?

○ Yes

○ No

○ N/A

○ Other

46. Are there certificates indicating that staff have been trained on the procedural and technical aspects of maintaining investigation records?

○ Yes

○ No

○ N/A

○ Other

47. Is there an actual log entry from an investigation showing detailed information on the actions performed, including data collection, analysis conducted, and conclusions drawn?

○ Yes

○ No

○ N/A

○ Other

48. Is there a summary from an internal audit focusing on the management of investigation records, detailing compliance with the policy and the effectiveness of the integrity protections?

○ Yes

○ No

○ N/A

○ Other

RESPOND Incident Management - RS.AN-07

Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved

49. Is there a comprehensive document that specifies how data should be collected, stored, and protected during and after an incident?

○ Yes

○ No

○ N/A

○ Other

50. Are there records or logs showing integrity checks or hash values calculated for collected data to ensure that it has not been altered from its original state?

○ Yes

○ No

○ N/A

○ Other

51. Are there summaries or agendas of training sessions dedicated to incident data collection and protection, showing what topics were covered and who attended?

○ Yes

○ No

○ N/A

○ Other

RESPOND Incident Response - RS.AN-08

An incident's magnitude is estimated and validated

52. Is there a section of the incident response plan that details the methodology for assessing the magnitude of incidents?

○ Yes

○ No

○ N/A

○ Other

53. Do incident reports include detailed magnitude estimates and the evidence or analysis used to validate these estimates?

○ Yes

○ No

○ N/A

○ Other

54. Are staff members trained in methods for estimating and validating the magnitude of incidents?

○ Yes

○ No

○ N/A

○ Other

55. Does audit review the practices for estimating and validating incident magnitudes, including any findings and recommendations for improvement?

○ Yes

○ No

○ N/A

○ Other

56. Are minutes from a review meeting documented where the magnitude of a particular incident was discussed, including any decisions made based on the estimated and validated magnitudes?

○ Yes

○ No

○ N/A

○ Other

RESPOND Incident Response Reporting and Communication - RS.CO-02

Internal and external stakeholders are notified of incidents

57. Does a policy document exists that specifies the guidelines for notifying internal and external stakeholders about incidents?

○ Yes

○ No

○ N/A

○ Other

58. Have relevant personnel been trained in the incident communication protocols?

○ Yes

○ No

○ N/A

○ Other

59. Have any audits been conducted that evaluated how well the organization communicates with external stakeholders during incidents?

○ Yes

○ No

○ N/A

○ Other

60. Is there any documentation that compiles feedback from stakeholders on the notification process used during a recent incident, highlighting areas of success and opportunities for improvement?

○ Yes

○ No

○ N/A

○ Other

RESPOND Incident Response Reporting and Communication - RS.CO-03

Information is shared with designated internal and external stakeholders

61. Is there a policy document that outlines the procedures for sharing information with internal and external stakeholders, including data sensitivity classifications and approved communication methods?

○ Yes

○ No

○ N/A

○ Other

62. Are there any meeting minutes from training sessions provided to staff on the proper handling and sharing of sensitive information?

○ Yes

○ No

○ N/A

○ Other

63. Have there been any internal audits reviewing the information sharing practices, noting any non-compliance issues and recommendations for enhancements?

○ Yes

○ No

○ N/A

○ Other

64. Is there any documentation on the feedback on the usefulness and appropriateness of the information received, including suggestions for improvement?

○ Yes

○ No

○ N/A

○ Other

RESPOND Incident Mitigation - RS.MI-01

Incidents are contained

65. List all the cybersecurity technologies that automatically perform containment actions. For example, anti-malware tools

66. Does HNE have third-party responders that perform containment actions on behalf of HNE?

○ Yes

○ No

○ N/A

○ Other

67. Does HNE have the capability to transfer compromised endpoints to a remediation VLAN?

○ Yes

○ No

○ N/A

○ Other

RESPOND Incident Mitigation - RS.MI-02

Activities are performed to prevent expansion of an event and mitigate its effects

68. Does HNE have the capability to perform automatic eradication actions?

○ Yes

○ No

○ N/A

○ Other

69. Does HNE allow a third-party the capability to perform automatic eradication actions?

○ Yes

○ No

○ N/A

○ Other

RECOVER Incident Recovery Plan Execution - RC.RP-01

The recovery portion of the incident response plan is executed once initiated from the incident response process

70. Is there documentation showing that the recovery team has completed specific training on the recovery procedures outlined in the incident response plan?

○ Yes

○ No

○ N/A

○ Other

71. Does the recovery log (or change ticket) outline actions taken during the recovery phase, such as system restorations, data validations, and security checks?

○ Yes

○ No

○ N/A

○ Other

72. Is there a summary document from a post-recovery that reviews how the recovery was executed and verifies the integrity and security of the restored systems?

○ Yes

○ No

○ N/A

○ Other

RECOVER Incident Recovery Plan Execution - RC.RP-02

Recovery actions are selected, scoped, prioritized, and performed

73. Is there a document that is followed that outlines the approach to recovery, including how to assess the impact of incidents and determine which systems or services are recovered first?

○ Yes

○ No

○ N/A

○ Other

74. Are their training sessions provided to recovery personnel, focusing on the methodology for recovery planning and execution?

○ Yes

○ No

○ N/A

○ Other

75. Is there evidence of how actions were prioritized and executed, including time stamps and personnel assignments?

○ Yes

○ No

○ N/A

○ Other

76. Is there documentation for post incident review that evaluates the selection, scope, prioritization, and execution of recovery actions, highlighting any gaps and recommendations?

○ Yes

○ No

○ N/A

○ Other

77. Is there an after action review (AAR) that analyzes the recovery process for a specific incident, evaluating the effectiveness of the recovery actions and lessons learned?

○ Yes

○ No

○ N/A

○ Other

RECOVER Incident Recovery Plan Execution - RC.RP-03

The integrity of backups and other restoration assets is verified before using them for restoration

78. Are backups verified for the integrity of the backups and the specific methods used for verification?

○ Yes

○ No

○ N/A

○ Other

79. Is there a verification process that identifies anomalies?

○ Yes

○ No

○ N/A

○ Other

80. Is there a process that handles anomalies?

○ Yes

○ No

○ N/A

○ Other

81. Are backups stored offline or are immutable?

○ Yes

○ No

○ N/A

○ Other

RECOVER Incident Recovery Plan Execution - RC.RP-04

Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms

82. Is there documentation on training sessions for staff involved in postincident reviews, detailing the curriculum and learning objectives?

○ Yes

○ No

○ N/A

○ Other

83. Is there a postincident report that evaluates how well critical functions were maintained during the incident and recommendations for operational improvements?

○ Yes

○ No

○ N/A

○ Other

84. Are there meeting minutes where postincident adjustments were discussed, showing the involvement of highlevel management in the decisionmaking process?

○ Yes

○ No

○ N/A

○ Other

RECOVER Incident Recovery Plan Execution - RC.RP-05

The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed

85. Are there guidelines for system restoration, integrity checks, and procedures for confirming normal operations?

○ Yes

○ No

○ N/A

○ Other

86. Are restored assets checked for indicators of compromise and remediation of root causes of the incident before production use?

○ Yes

○ No

○ N/A

○ Other

87. Are restored systems verified for correctness and adequacy before putting the restored system back online?

○ Yes

○ No

○ N/A

○ Other

RECOVER Incident Recovery Plan Execution - RC.RP-06

The end of incident recovery is declared based on criteria, and incident-related documentation is completed

88. Is there a declaration of the end of the incident recovery once the criteria are met?

○ Yes

○ No

○ N/A

○ Other

89. Are after-action report prepared that documents the incident itself, the response and recovery actions taken, and lessons learned?

○ Yes

○ No

○ N/A

○ Other

RECOVER Incident Response Communication - RC.CO-03

Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders

90. Is senior leadership regularly updated on recovery status and restoration progress for major incidents?

○ Yes

○ No

○ N/A

○ Other

91. Are protocols defined in contracts for incident information sharing between the organization and its 3rd Parties?

○ Yes

○ No

○ N/A

○ Other

92. Is there a coordination crisis communication between the organization and its critical 3rd Parties?

○ Yes

○ No

○ N/A

○ Other

RECOVER Incident Response Communication - RC.CO-04

Public updates on incident recovery are shared using approved methods and messaging

93. Is there a coordination crisis communication between the organization and its critical 3rd Parties?

○ Yes

○ No

○ N/A

○ Other

94. Are there documented breach notification procedures for recovering from a data breach incident?

○ Yes

○ No

○ N/A

○ Other

95. Are the steps taken to recover from the incident and to prevent a recurrence documented and shared with applicable internal and external parties?

○ Yes

○ No

○ N/A

○ Other