



NIST CSF Assessment

NIST CSF Respond Worksheet



CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Prepared for:
Your Client's Company
Prepared by:
YourIT Company



NIST CSF Respond Worksheet

1 - Response Planning (RS.RP)

1.1 - Response Plan

2 - Communications (RS.CO)

2.1 - Personnel Training

2.2 - Incident Reporting

2.3 - Information Sharing

2.4 - Coordination with Stakeholders

2.5 - Information Sharing with External Stakeholders

3 - Analysis (RS.AN)

4 - Improvements (RS.IM)

4.1 - Lessons Learned

4.2 - Response Strategy Updates

Response Planning (RS.RP)

1.1 - Response Plan

Does your organization have a written response plan? Please attach a copy of the response plan if available.

No

Communications (RS.CO)

2.1 - Personnel Training

Has your personnel been trained to know their roles and order of operations when a response is needed?

No

2.2 - Incident Reporting

Are incidents reported consistent with established criteria?

No

2.3 - Information Sharing

Is information shared consistent with response plans?

No

2.4 - Coordination with Stakeholders

Does coordination with stakeholders occur consistent with response plans?

No

2.5 - Information Sharing with External Stakeholders

Does voluntary information sharing occur with external stakeholders to achieve broader cybersecurity situational awareness?

No

Analysis (RS.AN)

3.1 - Incident Analysis

Review the organization's response plan or recent response plan execution to ensure the following analysis steps are incorporated and performed. Attach a copy of the response processes and procedures along with any documentation of recent response plan execution.

<input type="checkbox"/>	RS.AN-1: Notifications from detection systems are investigated
<input checked="" type="checkbox"/>	RS.AN-2: The impact of the incident is understood
<input type="checkbox"/>	RS.AN-3: Forensics are performed
<input checked="" type="checkbox"/>	RS.AN-4: Incidents are categorized consistent with response plans
<input type="checkbox"/>	RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)

3.2 - Incident Mitigation

Review the organization's response plan or recent response plan execution to ensure the following mitigation steps are incorporated and performed. Attach a copy of the response processes and procedures along with any documentation of recent response plan execution.

<input type="checkbox"/>	RS.MI-1: Incidents are contained
<input checked="" type="checkbox"/>	RS.MI-2: Incidents are mitigated
<input type="checkbox"/>	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks

Improvements (RS.IM)

4.1 - Lessons Learned

Do the response plans incorporate lessons learned?

No

4.2 - Response Strategy Updates

Were response strategies reviewed and updated within the past 90 days?

No