YourIT!
Your Logo Goes Here

NIST CSF Assessment

NIST CSF Respond Worksheet

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

NIST CSF Respond Worksheet

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.

☐	RS.AN-1: Notifications from detection systems are investigated
☑	RS.AN-2: The impact of the incident is understood
☐	RS.AN-3: Forensics are performed
☑	RS.AN-4: Incidents are categorized consistent with response plans
☐	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.

☐	RS.MI-1: Incidents are contained
☑	RS.MI-2: Incidents are mitigated
☐	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