

Thank you for completing the Cyber Resilience Review post-assessment questionnaire. For more information about this questionnaire or about the Cybersecurity Advisors Program, please contact Tara Brewer at cyberadvisor@hq.dhs.gov

Cybersecurity Motivation

What was your organization's motivation to participate in the CRR? (select all that apply)

- | | |
|---|---|
| <input type="checkbox"/> Validate a Finding | <input type="checkbox"/> Proactive Cybersecurity Assessment/Start of Improvement Effort |
| <input type="checkbox"/> Review Compliance | <input type="checkbox"/> Obtain Professional Third-Party Opinion of Cyber Defenses |
| <input type="checkbox"/> Response to Incident within Organization | <input type="checkbox"/> Response to Incident within Industry |
| <input type="checkbox"/> Reinforce Standards | <input type="checkbox"/> Other: |

Assessment Impact

In which of the following CRR domains has your organization planned, scheduled, or implemented at least one improvement?

N/A | Planned | Scheduled | Implemented

- Asset Management
- Controls Management
- Configuration and Change Management
- Vulnerability Management
- Incident Management
- Service Continuity Management
- Risk Management
- External Dependencies Management
- Training and Awareness Management

As a result of the CRR, has your organization...

Improved its allocation of its overall IT and/or cybersecurity budget?
Yes | No

Established or changed your targeted cybersecurity posture?
Yes | No

Shared cybersecurity information with external parties?
Yes | No

If Yes, what information is shared:

- Lessons Learned Best Practices Training Tips
 Other:

Leveraged the NIST Cybersecurity Framework?
Yes | No

Please provide a brief explanation for any improvements or changes listed above:

Quality of Assessment & Report

Did DHS establish expectations through CRR preparations? Yes | No

Strongly Agree Neither Agree nor Disagree Strongly Disagree Explanation:

The CRR report was comprehensible, readable, and usable.

The CRR report was valuable.

The CRR met my organization's expectations.

How could the CRR be improved?

How could the CRR report be improved?

Next Steps

Is your organization interested in participating in additional DHS cyber assessments or other services? (select all that apply)

A Re-Assessment of the Same Critical Service:

- Cyber Resilience Review (CRR)
- External Dependencies Management (EDM)
- Cyber Infrastructure Survey (CIS)

A New Assessment of a Different Critical Service:

- Cyber Resilience Review (CRR)
- External Dependencies Management (EDM)
- Cyber Infrastructure Survey (CIS)

Another DHS Service:

- Phishing Campaign Assessment
- Network Risk and Vulnerability Assessment
- Cybersecurity Evaluation Tool
- Industrial Control Systems Evaluation
- Cyber Hygiene Scanning