

IBM NIST CSF Assessment

Key Benefits

- Identify strengths and weaknesses for each cybersecurity area
- Helps your business prioritize cybersecurity projects
- Helps your business prepare for compliance and government regulations
- Roadmap to reach your desired cybersecurity maturity level by working with IBM specialists and technologies



Introduction

What is your level of cybersecurity maturity? What are your strengths and weaknesses? Are you ready for a network intrusion or security breach?

The **NIST CSF Assessment** is delivered by IBM Cybersecurity Experts who will focus on understanding your business objectives, business risks, regulatory compliance requirements and desired cybersecurity maturity level and review and assess the current state of your cybersecurity posture by reviewing roles and responsibilities, processes and deployment of tools.



By identifying strengths, gaps, opportunities for improvement in security practices and prioritizing recommended actions to be taken, your organization can meet your desired security maturity level and support a culture of continuous improvement.



IBM NIST CSF Assessment Delivery

IBM NIST CSF Assessment Delivery Phases*

Kick Off Planning 1 Day	Review objectives, explain the assessment methodology, set maturity levels desired and schedule interviews
Interviews and Data Collection 2 Days	Collect interviews data through digital whiteboard collaboration space
Analysis 3 Days	Analyze interview results and compare against maturity levels desired. Prepare results and key findings presentation, build the detailed report, and define your roadmap based on your goals
Reporting 3 Days	Present and provide Executive Briefing summarizing findings and roadmap

**A "High-level NIST CSF Assessment" can be performed based on the main NIST controls, with an estimated duration of 2 hours of interviews.*