



A NIST CSF-Aligned Portfolio for Ransomware

Backgrounder

The threat, costs, and impacts of ransomware continue to increase in magnitude and complexity, posing substantial challenges for IT security teams. At the same time there are best practices to reduce the risk of a ransomware incident, reduce response and recovery times, and minimize the impacts and costs of an incident.

Flexential experts know these best practices and provide many services to implement them successfully. Part of best practice is to leverage comprehensive industry frameworks and standards that have been created, curated, and proven to accomplish specified outcomes.

For the topic of cybersecurity, including ransomware, the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 (CSF) is an excellent framework “based on existing standards, guidelines, and practices to help organizations better manage and reduce cybersecurity risk.”

To support our customers with their cybersecurity and ransomware challenges, Flexential has mapped our services portfolio to the functions of the NIST Cybersecurity Framework. The result is a NIST CSF-Aligned portfolio of Flexential services that support customers with end-to-end best practice activities enabling organizations to identify, protect, detect, respond, and recover from cybersecurity threats and incidents—including ransomware—while complementing an organization’s existing standards, frameworks, and requirements.

Our NIST CSF-Aligned services portfolio includes over twenty services aligned to protecting against and detecting, responding, and recovering from cyber incidents. Customers choose services or programs that fit their specific requirements, compliance needs, desired outcomes, existing security posture, budget, and staffing levels. These services also support organizations in meeting their cyber insurance policy requirements.

When used together and with an organization’s internal efforts, these Flexential services strengthen our customers’ security posture, mature their cybersecurity program, increase cyber resiliency, and reduce ransomware risks.



About NIST

NIST is a federal agency within the United States Department of Commerce. NIST’s mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Since 1972, NIST has conducted cybersecurity research and developed cybersecurity guidance for industry, government, and academia.

NIST Cybersecurity Framework 2.0

The National Institute of Standards and Technology (NIST) promotes standards and advances technologies for innovation, industrial competitiveness, and improved quality of life. NIST is part of the U.S. Department of Commerce. Included in the many NIST publications is their cybersecurity framework.

The NIST Cybersecurity Framework 2.0¹ helps organizations of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data by providing a comprehensive set of best practices to prioritize cybersecurity activities. The NIST CSF is organized around six functions: Identify, Protect, Detect, Respond, Recover, and Govern.



- Identify threats, vulnerabilities and risk
- Protect by implementing safeguards
- Detect the occurrence of cybersecurity events
- Respond to detected events
- Recover and restore services
- Govern with oversight and visibility

Flexential services

Flexential has a wide array of services that align with each of the functions of the CSF 2.0. Our portfolio of services support organizations in advancing and maturing their cybersecurity program using proven best practices and industry standards that support quality, comprehensiveness, and faster implementations.

Flexential services can address every level of maturity and security posture and our engagements are tailored to individual customer needs to provide the most customer value. Additionally, the Flexential Cybersecurity Maturity Model can help to quickly assess maturity level and determine which activities and risks should be addressed first.

Whether your concern is ransomware, unplanned downtime, data loss, or your security posture, Flexential NIST CSF-aligned services strengthen protections and improve your identify, govern, detection, response, and recovery capabilities.

Contact us today for more information on how Flexential can help you reduce risk and advance your capabilities.

¹ [NIST Cybersecurity Framework 2.0 Resource & Overview Guide](#)

Flexential Ransomware Solution Portfolio

Identify

- Risk Assessments
- Security Assessments
- Cybersecurity Maturity Assessment
- Ransomware Defense Readiness Assessment
- DR Gap Analysis
- DR Strategy Workshop
- Penetration Testing
- Vulnerability Scanning
- Social Engineering

Protect

- DR Program Management
- DR Design & Planning
- DR Testing
- Managed Firewall
- Managed Web Application Firewall

Detect

- Cyber Defense Program
- Managed detection and response (MDR)

Respond

- IR Program Management
- IR Readiness Assessment

Recover

- Backup-as-a-Service
- Disaster Recovery-as-a-Service
- Managed Storage with tamperproof snapshots, and asynchronous volume replication

Govern

- Cybersecurity Program Development