FLEXENTIAL®

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 (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 complimenting 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 ransomware incidents. Customers choose services or programs that fit their specific requirements, compliance needs, desired outcomes, existing security posture, budget, and staffing levels. These services can 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, and reduce ransomware risks.

About NIST

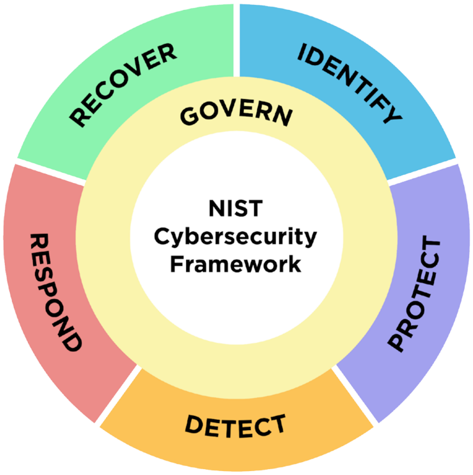
NIST is a federal agency within the United States Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

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

NIST Cybersecurity Framework

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 (CSF) 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 five functions: Identify, Protect, Detect, Respond, and Recover.



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

Flexential services

Flexential has a wide array of services that align with the entire NIST CSF, across each of the five functions. Our portfolio of services support organizations in advancing and maturing their cybersecurity program using proven best practices and industry standards that help ensure 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 quickly assess maturity level and help determine what type of activities and risks should be addressed first.

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

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

Flexential's ransomware solution portfolio

- Risk assessment
- Ransomware defense readiness assessment
- Cyber defense program
- Penetration testing
- Social engineering
- Managed detection and response (MDR)
- Managed firewall (IDPS/MFA/VPN)
- Managed web application firewall
- Incident response program management
- Disaster recovery strategy workshop
- Disaster recovery design and planning
- Disaster Recovery as a Service assisted testing
- Disaster Recovery as a Service managed testing
- Flexential Disaster Recovery as a Service
- Flexential Backup as a Service

[1] *NIST Cybersecurity Framework Quick Start Guide*