NIST
Cybersecurity Framework Success Story
SAP SE

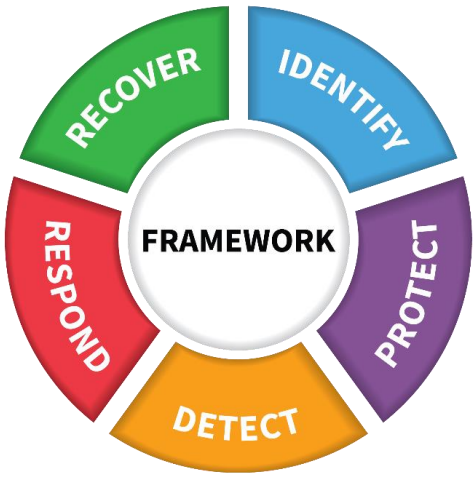
The voluntary Framework for Improving Critical Infrastructure Cybersecurity was developed through a collaborative process by industry, academia, and government stakeholders. It enables organizations – regardless of size, sector, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improve security and resilience. NIST does not validate or endorse any individual organization or its approach to using the Cybersecurity Framework.

Organizational Profile

SAP is a market leader in enterprise application software, offering companies of all sizes and in all industries Intelligence Enterprise solutions. With over 400,000 customers in over 180 countries, the SAP Group employs over 105,000 staff in over 140 countries. SAP's end-to-end suite of applications and services enables customers to operate profitably and to continuously adapt. In response to the ever-increasing rise in cybersecurity threats, SAP's Executive Board decided in 2019 to implement NIST CSF.

Situation

In a fast-evolving cyberthreat environment, we constantly review our cybersecurity and lead the way in developing new approaches to protecting our customers. For this reason, we've been working to strengthen our cybersecurity practices by implementing the NIST CSF, which helps us to strategically manage cybersecurity risk and make informed investment decisions.



Process

The NIST CSF implementation stretched over several years and was divided into five phases. In addition, throughout the implementation SAP has been directly collaborating and provisioning input regarding the NIST CSF to the NIST organization, including a review of the NIST CSF v2.0 with the new Govern function – prior to publication.

1. Initiation

With SAP's Executive Board making the strategic decision to implement the NIST CSF, the board recognized the need for it and its ability to integrate with SAP's existing frameworks (such as the ISO 31000, NIST SP800-30, etc.).

A program was initiated and led by a handpicked team of cybersecurity professionals to manage the implementation and coordinate the work across SAP globally, including engaging EY as a strong implementation partner.

2. Assessment

Prior to starting the implementation, an international IT audit organization assessed our existing cybersecurity measures. The assessment helped us establish our baseline security control maturity and prioritize focus areas for the framework implementation.

3. Pilot

For our pilot project, we selected three focus areas: risk management, third-party risk management, and business continuity management. During the eight-week project, we established ownership for all our security controls in each area.

4. Implementation

We ran a series of workshops with our IT and business leaders to define the blueprint for the overall implementation of company-wide security controls. As well as assigning future owners and defining each control step, the workshops also helped better connect our central services team with lines of business and other units across our complex organization.

Process (Continued)

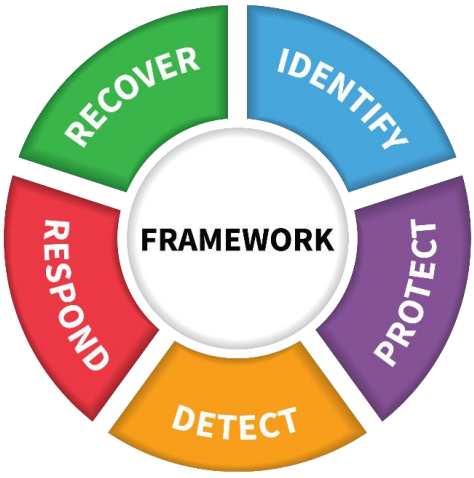
The implementation was tracked through project Key Performance Indicators (KPIs) applying a programmatic approach. When we finally reached all our milestones at the end of 2023 implementing the NIST CSF Tier 3 across all of SAP, including remediating all identified issues, the project was two months ahead of schedule.

5. Final quality check

At the conclusion of the project, a team from EY checked that we had carried out each stage of the implementation according to the project blueprint and assessed our alignment with the NIST CSF Tier 3 as well as confirmed that we had achieved it.

Results and Benefits (Continued)

For SAP, our NIST CSF implementation and achievement of Tier 3 has delivered several benefits. We now have a better understanding of our cybersecurity risks and are confident in our structured and systematic approach to managing them – with robust policies, strengthened governance, and more effective controls in place. In addition, the implementation process has fostered increased collaboration between our central IT services experts and different business teams across the company.



Results and Benefits (Continued)

The NIST CSF aided us in structuring our cybersecurity organization. Moreover, the framework unites our cybersecurity team in a common vision and gives visibility throughout all management levels of our cybersecurity risk, thereby enabling an ongoing dialogue about cybersecurity to help manage the risk throughout all layers of the organization.

Furthermore, our innovative self-assessment methodology has affirmed us in our journey to bolster our cybersecurity capabilities, importantly enabling us to proactively address emerging threats, bolstering the security of our products and services. This commitment to risk mitigation ultimately safeguards critical processes for our global customer base.

Contact Information & Resources

Vanessa Barber, vanessa.barber@sap.com
Daniel Fryer, daniel.fryer@sap.com
Kathrin Becker, kathrin.r.becker@de.ey.com
Peter Westphal, peter.westphal@de.ey.com
Brochure - Click here

NIST Cybersecurity Framework Website:
https://www.nist.gov/cyberframework

NIST Contact: cyberframework@nist.gov