This case study is fictional and notional, not intended to represent any real company, and for discussion purposes only.

NOTIONAL Fictional Case Study: Company A

Company A seeks to use the Cybersecurity Framework by leveraging guidance and approaches to improve its cybersecurity and cyber resilience.

- Company A is a company founded in 1965, which provides services to 500,000 customers and employs 8,000 workers throughout the Midwest.
- Prior to using the CSF, Company A's approach to cybersecurity risk management included complying with sector regulations. Its risk management processes are integrated into its core business functions.
- Company A is an active member of its Sector Coordinating Council and the Cross Sector Cyber Security Working Group (CSCSWG).

The following recommended steps illustrate how an organization could use the CSF to create a new cybersecurity program or improve an existing cybersecurity program.

Recommended CSF Steps	
Step 1: Identify.	The organization identifies its mission objectives, related systems and assets, regulatory requirements and overall risk approach
Step 2: Create a Current Profile.	Beginning with the Categories specified in the Framework Core, the organization develops a Current Profile that reflects its understanding of its current cybersecurity outcomes based on its adoption of the Identify Function
Step 3: Conduct a Risk Assessment.	The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization
Step 4: Create a Target Profile.	The organization creates a Target Profile that focuses on the assessment of the Framework Elements (e.g., Categories, Subcategories) describing the organization's desired cybersecurity outcomes
Step 5: Determine, Analyze, and Prioritize Gaps.	The organization compares the Current Profile and the Target Profile to determine gaps, and then determines resources necessary to address the gaps
Step 6: Implement Action Plan.	The organization implements the steps defined in the action plan and monitors its current cybersecurity practices against the Target Profile

CSF Use Scenario

- Company A performed a self-evaluation and determined it currently meets all the descriptions in CSF Tier 2. This self-evaluation included determining the company's defined, institutionalized, risk-informed, and management-approved processes and procedures.
- Company A decides it will work towards meeting CSF Tier 3. The company identified its target tier by comparing current risk management activities and current sector cybersecurity regulations to the CSF to identify gaps and areas for improvement.
- Areas for improvement for Company A were based on current profile, target profile, and industry stakeholder input that focused on improving critical areas of cybersecurity and resilience. These areas included authentication, data analysis, privacy standards, and supply chain risk management.

This case study is fictional and notional, not intended to represent any real company, and for discussion purposes only.

Bolded text below represents CSF Core Function Areas that Company A chooses to pursue as areas for improvement:

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
•Asset Management •***Business Environment*** •Governance •Risk Assessment •Risk Management Strategy	•Awareness and Training •Data Security •***Information Protection Processes and Procedures*** •***Protective Technology***	•***Anomalies and Events*** •***Security Continuous Monitoring*** •***Detection Processes***	•***Response Planning*** •Communications •***Analysis*** •***Mitigation*** •***Improvements***	•***Recovery Planning*** •***Improvements*** •Communications