NIST Cybersecurity Framework
A framework for safeguarding data and protecting our organization.
WHAT IS THE NIST CSF?
The NIST Core describes the cybersecurity activities and outcomes you’ll help us accomplish by implementing the Framework.

The Core is multi-disciplinary, so it’s easy to understand regardless of technical background—but it’s also robust. The examples here are just an introduction.

To learn more, click CSF Core Components. When you are finished, click Next.
CSF Core Components

Functions

- At its highest level the CSF is organized into 5 Functions: Identify, Protect, Detect, Respond, and Recover.
- Each Function addresses a variety of risks organizations may encounter.
- Don't think about this as a linear process; the Functions are performed concurrently and continuously to form an operational culture that addresses dynamic cybersecurity risk.

Click any FUNCTION to learn more about how these activities are organized.
Within each Category are many Subcategories, 108 in total, that describe the outcomes that will benefit our organization when implemented.

**FUNCTION**
- IDENTIFY
- PROTECT
- DETECT
- RESPOND
- RECOVER

**CATEGORIES**
- Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
- Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is

**SUBCATEGORIES**
- ID.BE-1: The organization's role in the supply chain is identified and communicated
- ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated
- ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated
- ID.BE-4: Dependencies and critical functions for delivery

Explore the various FUNCTIONS, CATEGORIES, and SUBCATEGORIES as desired. When you are finished, click NEXT.
A lot goes into implementing the CSF, and you may not always see the benefits until they're really needed.

Think of the planning you do now like an investment which will help protect us in the future.

Let's see what could happen as a result of implementing ... or not implementing, each Function of the CSF.

To learn more about FUNCTIONS, click the characters above. When you're finished, click NEXT.
Identify

Nick's a desktop support specialist who's service area is infected by malware from a spear phishing attack. Nick has no idea how many resources might be compromised, or what business functions are put at risk. Nick doesn't even know how to properly report the incident!

Click IMPLEMENT the CSF!

To learn more about FUNCTIONS, click the characters above. When you're finished, click NEXT.
Implementation Tiers describe how well we align with the characteristics in the NIST Cybersecurity Framework. Tiers are numbered 1-4. The more we align, the higher our Tier.

Tiers are important because they measure our cybersecurity triumphs, opportunities, and goals.

Applying Tiers to our business isn’t a pass or fail judgement; it’s a marker of how well we’re doing, and where we want to go.
We've just touched on some of the most important components of NIST's cybersecurity Framework.

Implementing the CSF's various actions and desired outcomes is up to you.

The details depend on your job role. No one person can implement the entire Framework; it takes a team of skilled professionals from across our organization.

This activity is optional. If you have a moment, see which CSF Functions apply most to your role. Or click Next to continue to the course Summary and the course completion.