You’re new to security so Heidi is going to take a few minutes to explain the NIST Cybersecurity Framework to you.

Essentially, you learn that NIST Cybersecurity Framework divides cybersecurity into 5 different functions:

* Identify: Identification, inventory, assessment, and governance of enterprise assets and related risks.
* Protect: What is important to protect, why protection is necessary, and what protections are prudent to guard against any entity that could use our data in inappropriate ways.
* Detect: Deployment and management of capabilities designed to monitor for potential security incidents.
* Respond: Analysis, implementation, and maintenance of methods to address and minimize impacts of security incidents.
* Recover: Maintaining or returning the business to normal operations following security incidents.

*NIST Cybersecurity Framework has five maturity tiers, which can be used for current state scoring: Tier 0: Non-existent, Tier 1: Partial, Tier 2: Risk-Informed, Tier 3: Repeatable and Tier 4: Adaptive.*

Brief explanation of different tiers:

* Tier 0: does not exist
* Tier 1: ad-hoc or heavily relying on individual's knowledge
* Tier 2: decentralized or there are only informal processes
* Tier 3: company-wide, documented processes
* Tier 4: innovative technologies in use, proactive review and development

For further information: <https://www.nist.gov/cyberframework>

Save this information, as you’ll use it in the next part