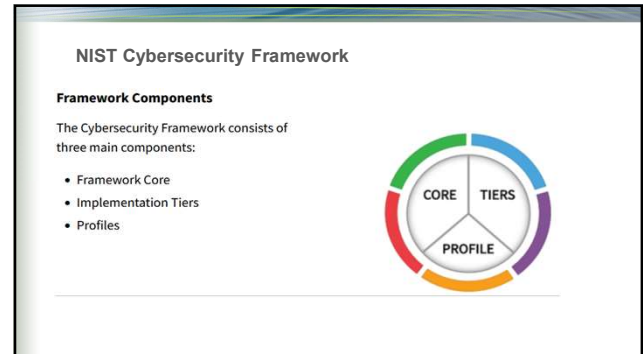
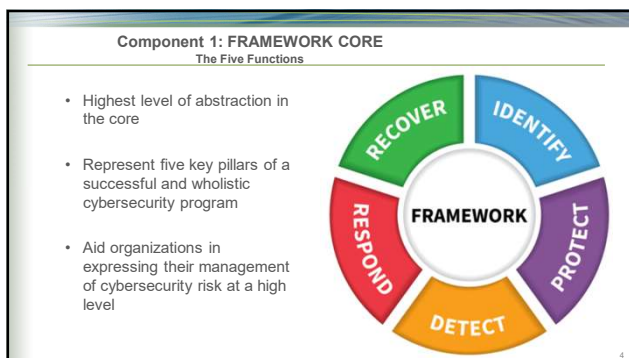


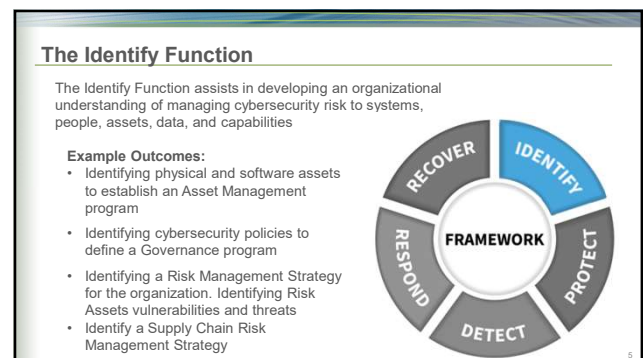
2



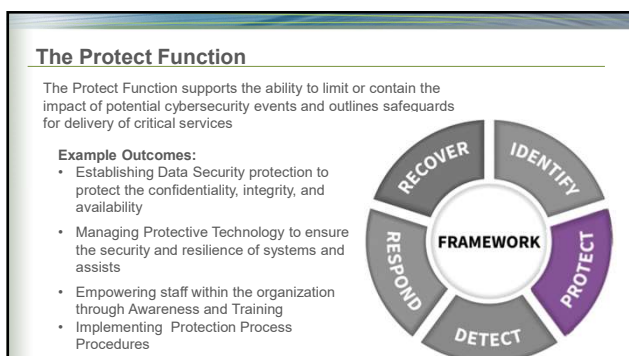
3



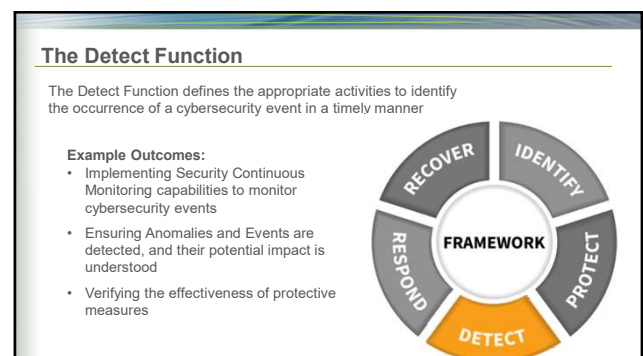
4



5



6



7

The Respond Function

The Respond Function includes appropriate activities to take action regarding a detected cybersecurity incident to minimize impact

Example Outcomes:

- Ensuring Response Planning processes are executed during and after an incident
- Managing Communications during and after an event
- Analyzing effectiveness of response activities.
- Implement improvements



8

The Recover Function

The Recover Function identifies appropriate activities to maintain plans for resilience and to restore services impaired during cybersecurity incidents

Example Outcomes:

- Ensuring the organization implements Recovery Planning processes and procedures
- Implementing improvements based on lessons learned
- Coordinating communications during recovery activities



9

Examples

Protect	Implement a monthly information security email newsletter informing the recipients of current threats to the organization and its personnel.
Identify	Build a comprehensive inventory of all systems, including hardware and software.
Recover Improvement	Ensure that each time a plan is implemented that lessons learned are incorporated back into the plan.
Detect	Establish a baseline of known normal behaviors to identify anomalies and events.
Recover comm	Engage public relations to ensure efforts are communicated internally and externally.

10

Summary



11

Component 2: Implementation Tiers

- The CSF is designed to be useful for all areas of the industry.
- Implementation tiers aid that mission by providing multiple tiers based on your organization risks appetite
- The NIST CSF describes 4 Tiers to aid in implementation
- Tiers are tools to help the organization identify decisions regarding cybersecurity
- Think of Tiers as the preferred outcome of activity

Cybersecurity Framework Tiers



12

Tier 1 - Partial:
Reactive to situations
No formalized security process
Does not participate in any information sharing activities

Tier 2 - Risk Informed:
Policies may exist, but are known to only a few key people
Threats are recognized, but may not be efficiently communicated to even internal parties
Acts upon risks based on external intelligence, but probably not consistently

Tier 3 - Repeatable:
Organization has implemented CSF standards
Has formal policy that is updated on a regular basis
Organization can repeatedly respond to cyber crises

Tier 4 - Adaptive:
Can quickly adapt to new and emerging threats
Understands their place in the cyber supply chain and actively works to protect others
Risk management is built into culture so everyone is able to recognize risk

13

Component 3: Profiles

Profiles are both outlines of an organization's current cybersecurity status and roadmaps toward CSF goals for protecting critical infrastructure. NIST said having multiple profiles—both current and goal—can help an organization find weak spots in its cybersecurity implementations and make moving from lower to higher tiers easier.

Profiles also help connect the functions, categories and subcategories to business requirements, risk tolerance and resources of the larger organization it serves. Think of profiles as an executive summary of everything done with the previous three elements of the CSF.

14

Implementing a Cybersecurity Framework

Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7
--------	--------	--------	--------	--------	--------	--------

Step 1: Prioritize and Scope

This is where you determine the risk tolerance of the organization. It is at this point that you should decide which business processes need the most protection and should be considered in scope for this cycle. You can use different priorities on each area to address the unique needs of the organization.

Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7
--------	--------	--------	--------	--------	--------	--------

Step 2: Orient

Identify the threats and vulnerabilities that apply to the assets identified as in scope.

15

Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7
--------	--------	--------	--------	--------	--------	--------

Step 3: Create a Current Profile

Assign a tier number to each category and subcategory in the Framework. Remember, we aren't scoring ourselves on compliance, we are assessing our operational abilities. Usually whole numbers are good, but if you are fine tuning an area, maybe using half numbers for partial achievements will help.

Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7
--------	--------	--------	--------	--------	--------	--------

Step 4: Conduct a Risk Assessment

This is where you evaluate your organization's operational procedures to evaluate how well your current procedures mitigate the impact of known and emerging threats.

Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7
--------	--------	--------	--------	--------	--------	--------

Step 5: Create a Target Profile

Using the same implementation tiers as in your current profile, now is the time to determine where your organization's desired outcomes should be. This is also the time to consider outside influence of suppliers as well as external requirements of your customers and regulators.

16

Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7
--------	--------	--------	--------	--------	--------	--------

Step 6: Determine, Analyze, and Prioritize Gaps

Now is time to find the largest gaps in between the current and desired target profiles. This includes determining available resources and the business processes that need to be adjusted to accommodate the protection levels desired. It just doesn't make business sense to spend a million dollars protecting data that is only worth a hundred. A heatmap may help visualize this step.

Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7
--------	--------	--------	--------	--------	--------	--------

Step 7: Implement Action Plan

It's almost time to see progress! Now is the time to put your plan into action and start the transformation in motion.

This all becomes second-nature and develops into a repeatable process with practice and deployment. Annual cycles are adequate for most organizations, but you should customize to your needs and goals. Some start out as a monthly process and gradually stretch out as high-priority items are folded into the continuous cycle. Remember, this requires constant and consistent communication with all stakeholders regarding the current and desired tiers for your organization.

17