University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST Risk Management Framework

CS 4950
Homeland Security & Cybersecurity

Lesson 17
NIST
Risk Management Framework

Rick White, Ph.D.
University of Colorado, Colorado Springs

1
Esc

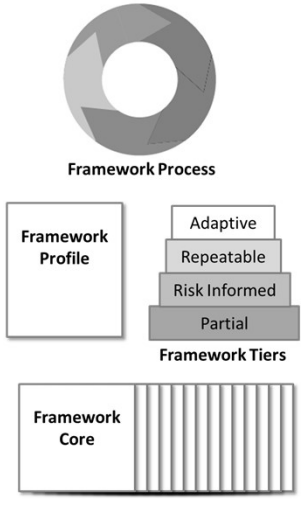
1

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST Cybersecurity Framework

- The NIST Cybersecurity Framework is a risk-based approach to managing cybersecurity.
- It is composed of four parts:
  1. Framework Core
  2. Framework Tiers
  3. Framework Profiles
  4. Framework Process

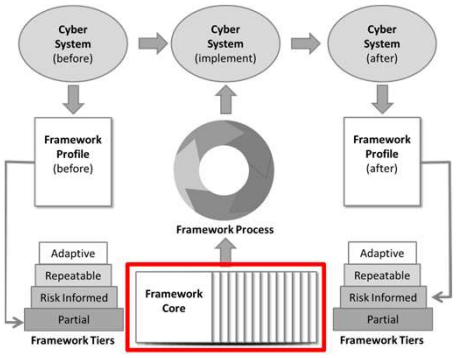


2
Esc

2

NIST Cybersecurity Framework

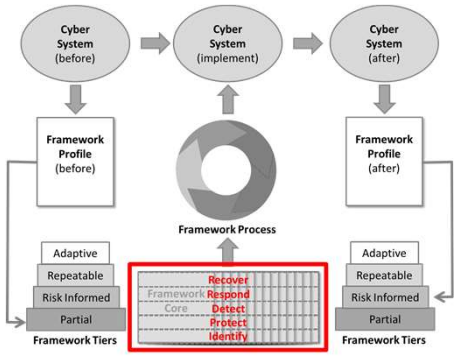
The **Framework Core** is a set of cybersecurity activities, desired outcomes, and applicable references that are common across infrastructure sectors.



3

NIST Cybersecurity Framework

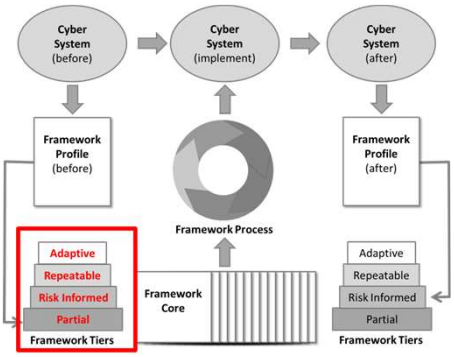
- The Framework Core consists of five concurrent and continuous **functions**: Identify, Protect, Detect, Respond, and Recover.
- Each of these functions is comprised of corresponding **categories** and **subcategories** of activities that are matched with a set of six separate **standards** and guidelines.



4

NIST Cybersecurity Framework

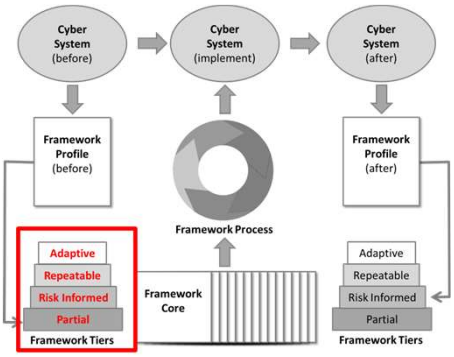
The **Framework Tiers** are conceptual targets representing four increasing levels of protection: 1) Partial, 2) Risk Informed, 3) Repeatable, and 4) Adaptive.



5

NIST Cybersecurity Framework

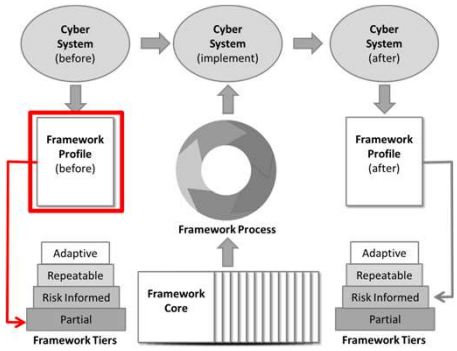
- Each Tier is characterized by three organizational attributes:
  1. The robustness of the risk management process
  2. The degree to which the risk management program is integrated within the organization, and
  3. The degree to which the risk management program is integrated with external partners.



6

NIST Cybersecurity Framework

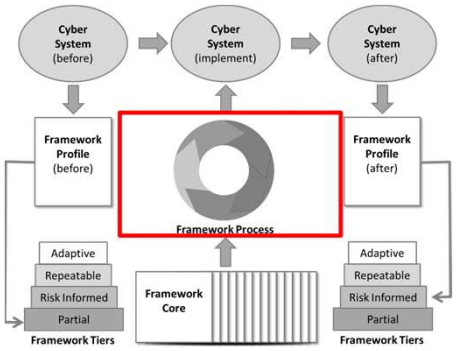
A **Framework Profile** is an assessment of the organization's tier level based upon the degree to which it currently conforms to the Framework Core.



7

NIST Cybersecurity Framework

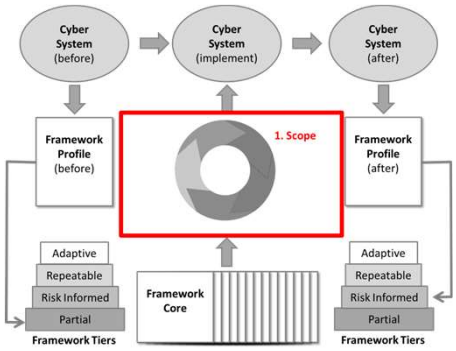
- The **Framework Process** employs the Framework Core, Framework Tiers, and Framework Profiles in a seven-step process to incrementally achieve increasing levels of protection.
- The Framework Process is a **collaborative process** between System Operators and Business Managers.



8

NIST Cybersecurity Framework

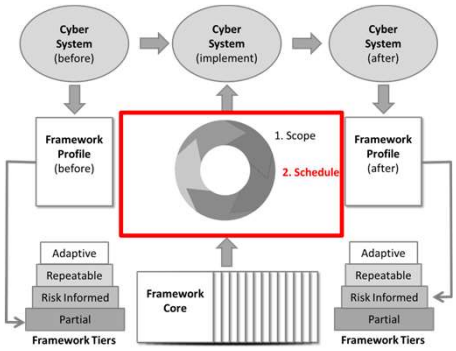
Step 1 establishes the scope and priority of the cybersecurity effort with respect to the goals and priorities of the organization.



9

NIST Cybersecurity Framework

Step 2 establishes the program schedule, phases, and milestones of the current round of effort.



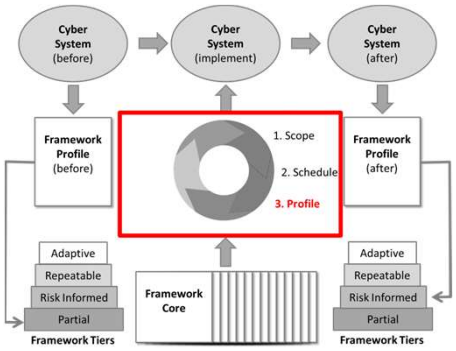
10

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST Cybersecurity Framework

Step 3 develops or updates the current Framework Profile.



11

Esc

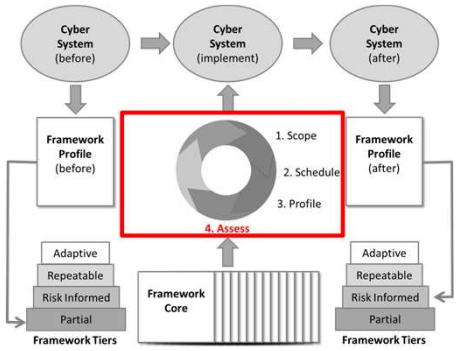
11

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST Cybersecurity Framework

Step 4 assesses the organization's current risk exposure based on its current profile.



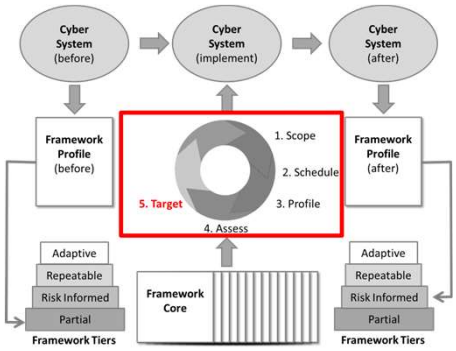
12

Esc

12

NIST Cybersecurity Framework

Step 5 creates a Target Profile based on the Framework Tier the organization chooses to attain.

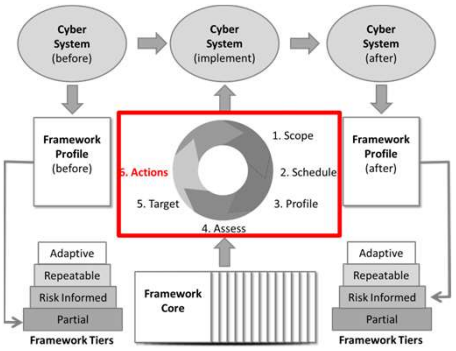


13
Esc

13

NIST Cybersecurity Framework

Step 6 identifies and prioritizes what Framework Core actions need to be done in order to attain the selected Target Profile.

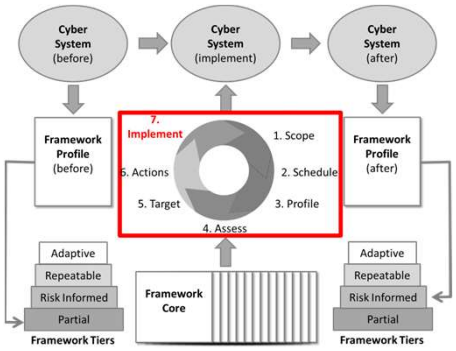


14
Esc

14

NIST Cybersecurity Framework

In Step 7 the organization undertakes the identified action in the designated priority order to attain the selected Target Profile.



15

Esc

15

NIST Cybersecurity Framework

Of course, all this is easier said than done.

16

Esc

16

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST Cybersecurity Framework

1. To begin, the Framework Core is **not a simple checklist.**
2. The recommended standards and guidelines consist of **hundreds of recommended actions**, some simple, some complex, some overlapping, and some that won't apply to your system.
3. **It'll take significant time and effort to build a checklist tailored to your system.**
4. Additionally, the **amount of effort required for each action will have to be costed** in a way that management can assess the return on investment and determine their individual risk reward.
5. Moreover, there's **no simple mapping** between the Framework Core and the Framework Tiers.
6. **The Framework Tiers will have to be defined** with respect to the Framework Core in a manner that makes sense for your organization.

17

Esc

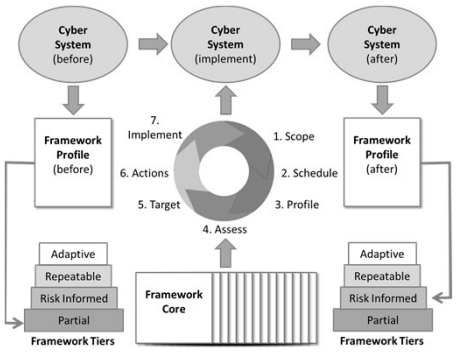
17

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST Cybersecurity Framework

The NIST Cybersecurity Framework requires a significant commitment in time and resources on the part of an organization.



18

Esc

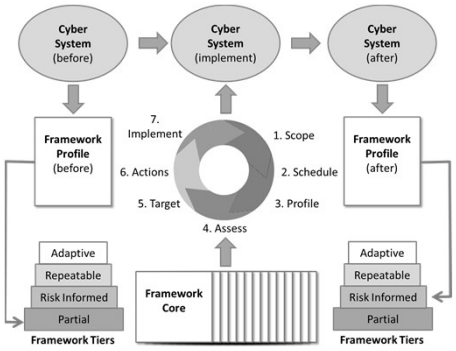
18

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST Cybersecurity Framework

The basic advantage, however, is it provides a systematic means of measuring your current status and progress towards a defined goal.



19

Esc

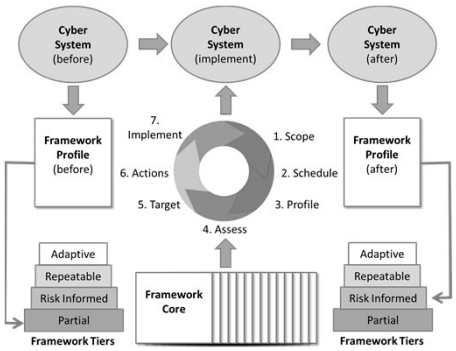
19

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST Cybersecurity Framework

Knowing where you are and where you're going is essential to developing a risk-based strategy consistent with the organization's mission and goals.



20

Esc

20

NIST Cybersecurity Framework

The alternative is to flounder without knowledge or direction of your exposure.

That indeed is the highest risk strategy of all.

21

Conclusion

Questions?

22