

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

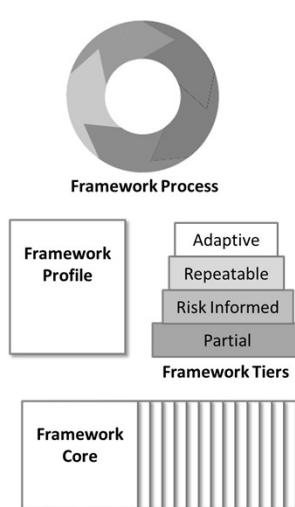


University of Colorado
Colorado Springs

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

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST Cybersecurity Framework

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

The diagram illustrates the NIST Cybersecurity Framework. At the center is the **Framework Core**, which is a set of cybersecurity activities, desired outcomes, and applicable references. This core is supported by **Framework Tiers**, which are categorized into four levels: Adaptive, Repeatable, Risk Informed, and Partial. The Framework Core is shown as a central box with a red border. The Framework Tiers are represented by a stack of boxes below the core. The Framework Process is shown as a cycle connecting the **Framework Profile (before)** and **Framework Profile (after)** states. The process involves the **Cyber System (before)**, **Cyber System (implement)**, and **Cyber System (after)** states. The Framework Process is shown as a cycle connecting the before and after states.

3 Esc

3

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

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.

The diagram illustrates the NIST Cybersecurity Framework. At the center is the **Framework Core**, which is a set of cybersecurity activities, desired outcomes, and applicable references. This core is supported by **Framework Tiers**, which are categorized into four levels: Adaptive, Repeatable, Risk Informed, and Partial. The Framework Core is shown as a central box with a red border. The Framework Tiers are represented by a stack of boxes below the core. The Framework Process is shown as a cycle connecting the **Framework Profile (before)** and **Framework Profile (after)** states. The process involves the **Cyber System (before)**, **Cyber System (implement)**, and **Cyber System (after)** states. The Framework Process is shown as a cycle connecting the before and after states.

4 Esc

4

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

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.

The diagram illustrates the NIST Cybersecurity Framework process. It shows a cycle starting with 'Cyber System (before)', moving to 'Cyber System (implement)', and then to 'Cyber System (after)'. Below each stage is a 'Framework Profile' (before, implement, after). A central 'Framework Process' is represented by a circular arrow. At the bottom, the 'Framework Core' is shown as a series of vertical bars. On either side of the core are 'Framework Tiers' stacks, each containing four levels: Adaptive (top), Repeatable, Risk Informed, and Partial (bottom). The left stack is highlighted with a red box. A small '5' and 'Esc' button are in the bottom right corner.

5

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST Cybersecurity Framework

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

The diagram is identical to the one on slide 5, showing the NIST Cybersecurity Framework process cycle and the Framework Tiers (Adaptive, Repeatable, Risk Informed, Partial) and Framework Core. A small '6' and 'Esc' button are in the bottom right corner.

6

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

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 Esc

7

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

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 Esc

8

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

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 Esc

9

UCCS University of Colorado
Colorado Springs

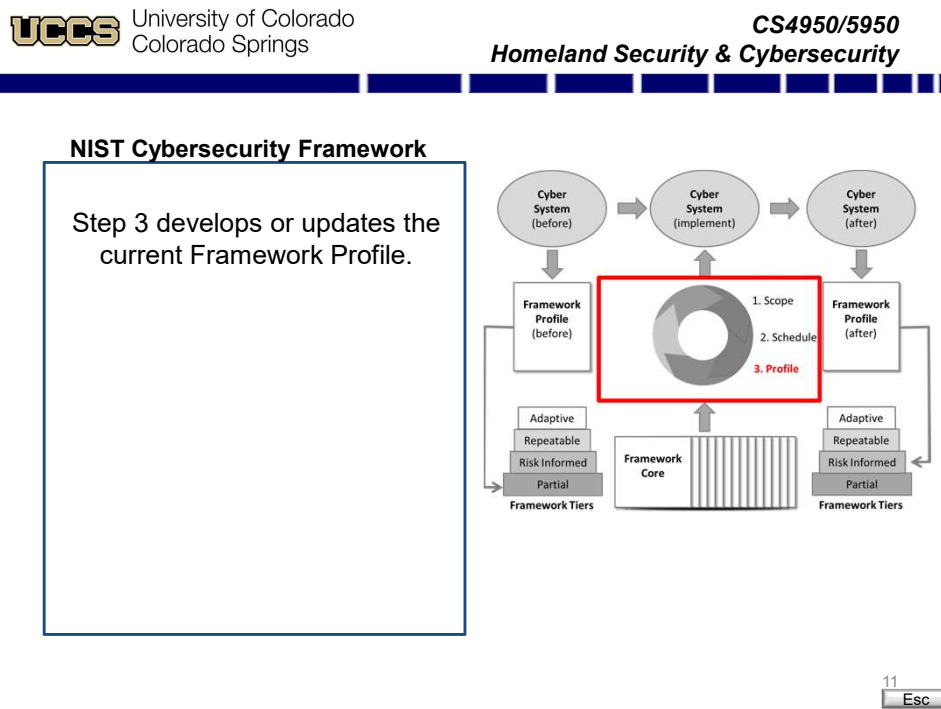
CS4950/5950
Homeland Security & Cybersecurity

NIST Cybersecurity Framework

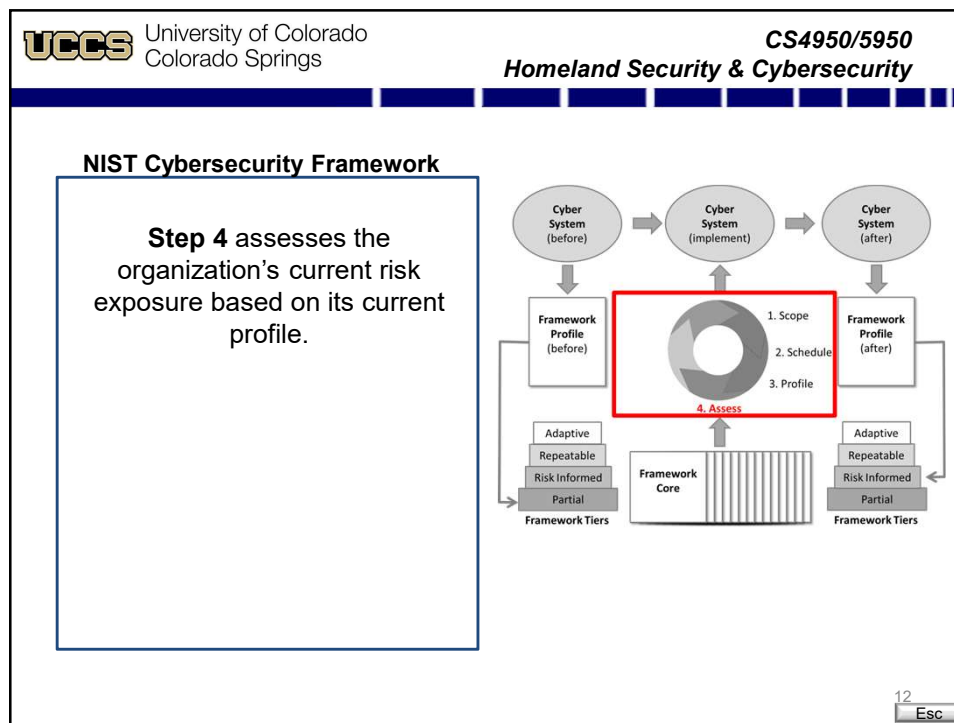
Step 2 establishes the program schedule, phases, and milestones of the current round of effort.

10 Esc

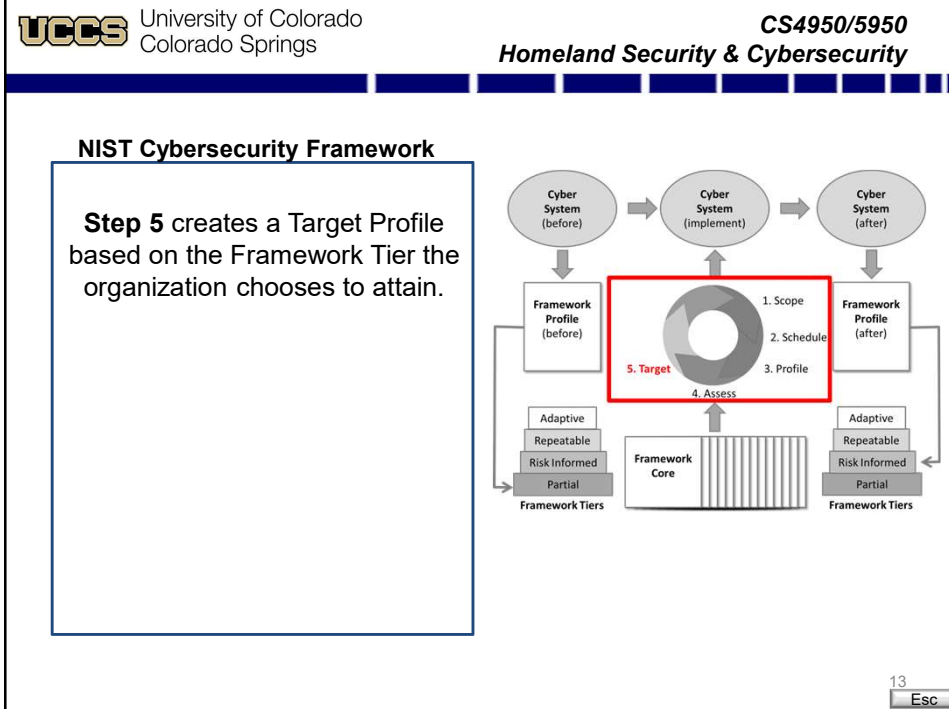
10



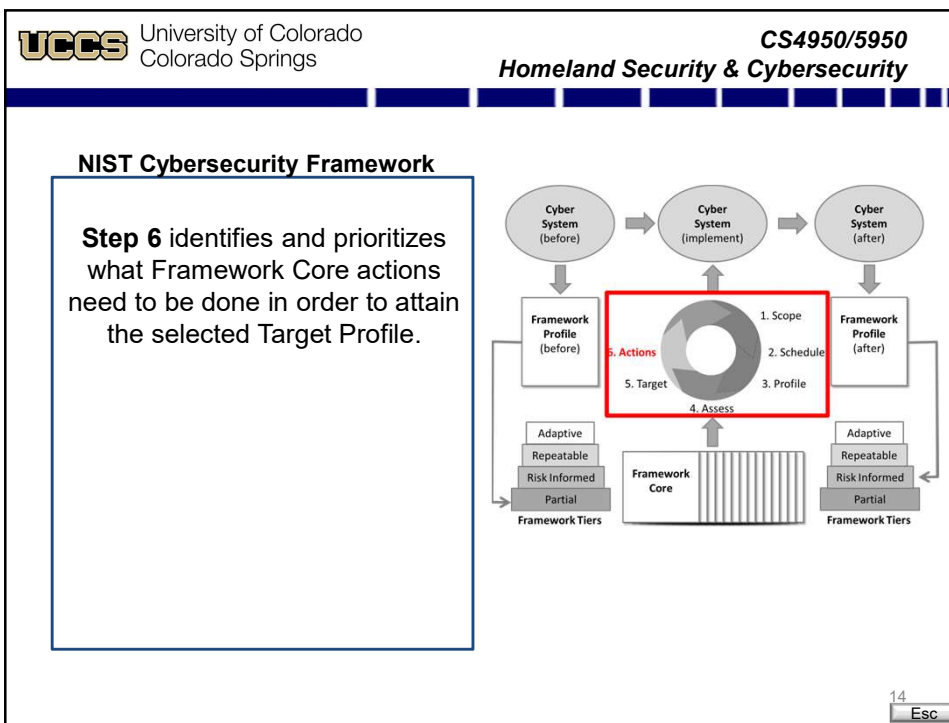
11



12



13



14

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

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

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST Cybersecurity Framework

Of course, all this is easier said than done.

16 Esc

16



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

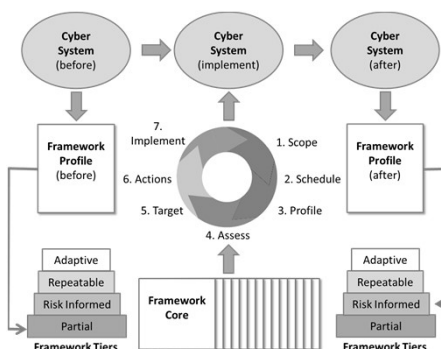
Esc

17



NIST Cybersecurity Framework

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



18

Esc

18

UCCS 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.

The diagram illustrates the NIST Cybersecurity Framework process. It shows a cycle starting with 'Cyber System (before)', moving to 'Cyber System (implement)', and finally to 'Cyber System (after)'. Below these, 'Framework Profile (before)' and 'Framework Profile (after)' are shown. The central part of the diagram is a circular flow with seven steps: 1. Scope, 2. Schedule, 3. Profile, 4. Assess, 5. Target, 6. Actions, and 7. Implement. Below this cycle is the 'Framework Core', which is a grid of 19 categories. To the left and right of the core are 'Framework Tiers', which are categorized as Adaptive, Repeatable, Risk Informed, and Partial. The entire process is framed by a blue border.

19 Esc

19

UCCS 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.

The diagram illustrates the NIST Cybersecurity Framework process. It shows a cycle starting with 'Cyber System (before)', moving to 'Cyber System (implement)', and finally to 'Cyber System (after)'. Below these, 'Framework Profile (before)' and 'Framework Profile (after)' are shown. The central part of the diagram is a circular flow with seven steps: 1. Scope, 2. Schedule, 3. Profile, 4. Assess, 5. Target, 6. Actions, and 7. Implement. Below this cycle is the 'Framework Core', which is a grid of 19 categories. To the left and right of the core are 'Framework Tiers', which are categorized as Adaptive, Repeatable, Risk Informed, and Partial. The entire process is framed by a blue border.

20 Esc

20


UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

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 Esc


21

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Conclusion

Questions?



22 Esc

22