

UCCS University of Colorado
Colorado Springs


CS4950/5950
Homeland Security & Cybersecurity

NIST RMF Exercise 1

CS 4950/5950
Homeland Security &
Cybersecurity

Lesson 18
NIST RMF
Exercise 1

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



1
Esc


1

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity


NIST CSF Exercise 1

You are the System Security
Officer for a drinking water facility
that provides 80% of the water for
a medium sized city of about
450,000 residents in Colorado.



2
Esc

2

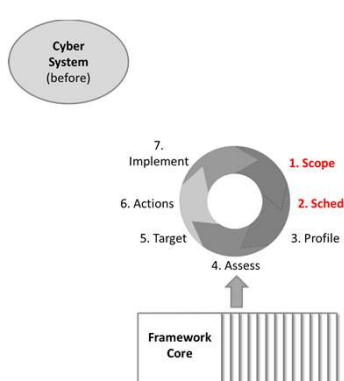


University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity


NIST CSF Exercise 1

Let's say that you've already met with senior management and agreed to make our first attempt at employing the NIST Cybersecurity Framework over the next year, in essence completing steps 1 and 2 of the System Framework.



3
Esc

3

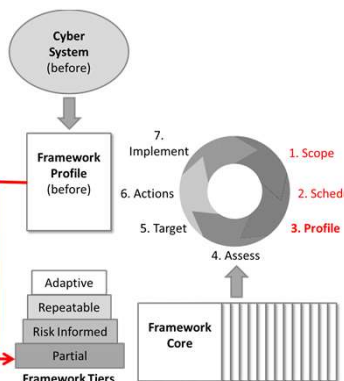


University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity


NIST CSF Exercise 1

- You're now six months into the project and developed a Current Profile using the Framework Core according to Step 3.
- According to our analysis, you rate the plant at Tier 1, "Partial", indicating that your risk management process has not previously been formalized, there has been no organization-wide approach to managing cybersecurity risk, and you have not included your suppliers in any past risk assessments.



4
Esc

4

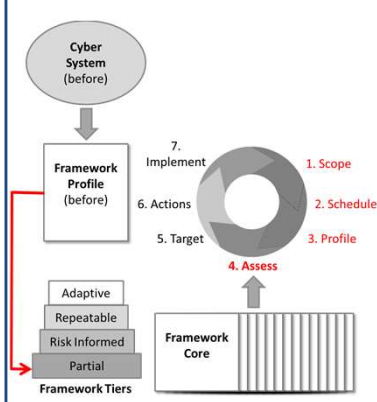


University of Colorado
 Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST CSF Exercise 1


- That puts you up to Step 4, conduct a risk assessment.
- You know there is a very low, but non-zero probability of malicious cyber attack that could disrupt 100% of the utility's service for up to a week.



The diagram illustrates the NIST CSF Framework. It shows a cycle of seven steps: 1. Scope, 2. Schedule, 3. Profile, 4. Assess, 5. Target, 6. Actions, and 7. Implement. A 'Cyber System (before)' leads into the 'Framework Profile (before)'. The 'Framework Tiers' are shown as a stack: Adaptive, Repeatable, Risk Informed, and Partial. The 'Framework Core' is represented by a grid. A red arrow points from the 'Partial' tier to the 'Assess' step.

5
 Esc

5

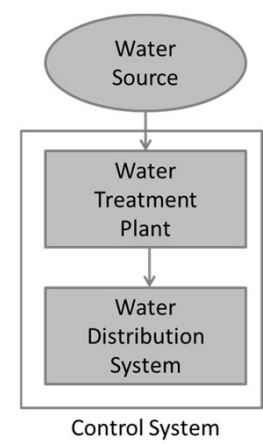


University of Colorado
 Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST CSF Exercise 1

Question: Is your current cybersecurity profile sufficient, or should you take the next step and try to achieve Tier Level 2?



The diagram shows a 'Water Source' leading to a 'Water Treatment Plant', which then leads to a 'Water Distribution System'. These three components are grouped within a box labeled 'Control System'.

6
 Esc

6

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST CSF Exercise 1

Given the circumstances in this example, that the utility supplies drinking water to 80% of 450,000 residents, **“Yes”, you should try to attain at least the next tier level, Tier Level 2.**

7
Esc

7

UCCS University of Colorado
Colorado Springs

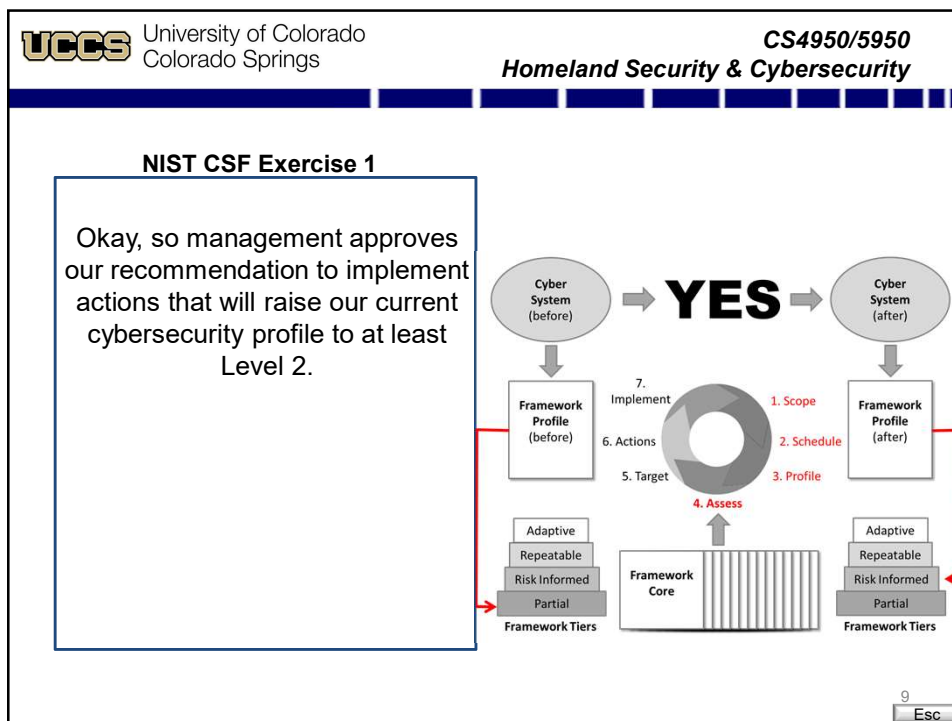
CS4950/5950
Homeland Security & Cybersecurity

NIST CSF Exercise 1

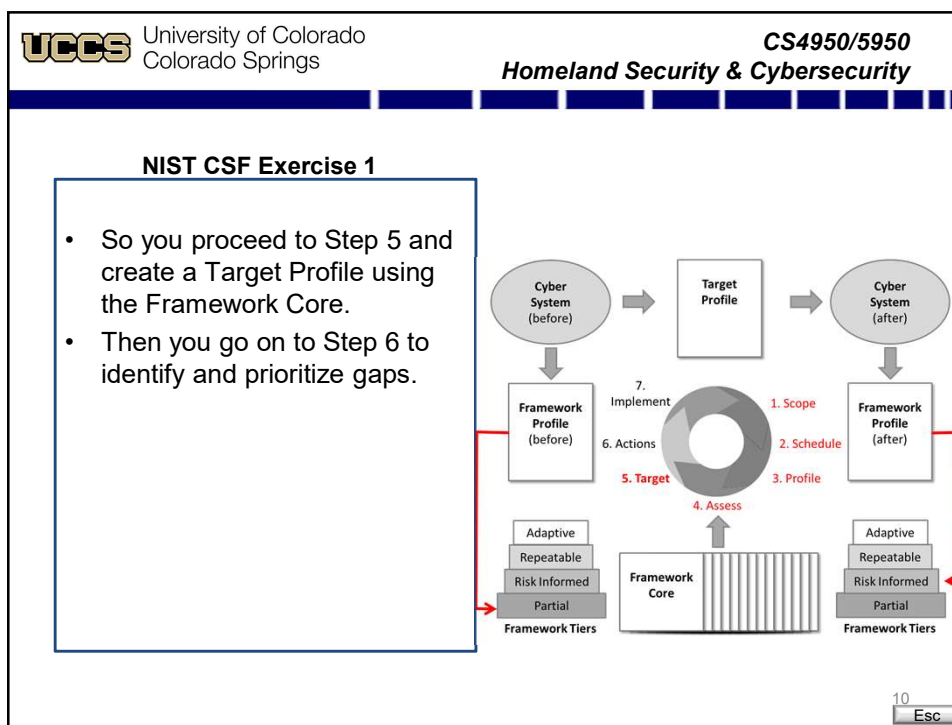
- Consider that you are looking at losing not only your drinking water supply, but also **pressure to your fire hydrants.**
- Government, businesses, and schools might have to shut down.**
- The **National Guard** might have to be called in to help set up points of distribution for drinking water.
- I hope you agree that such a situation would be considered catastrophic.**

8
Esc

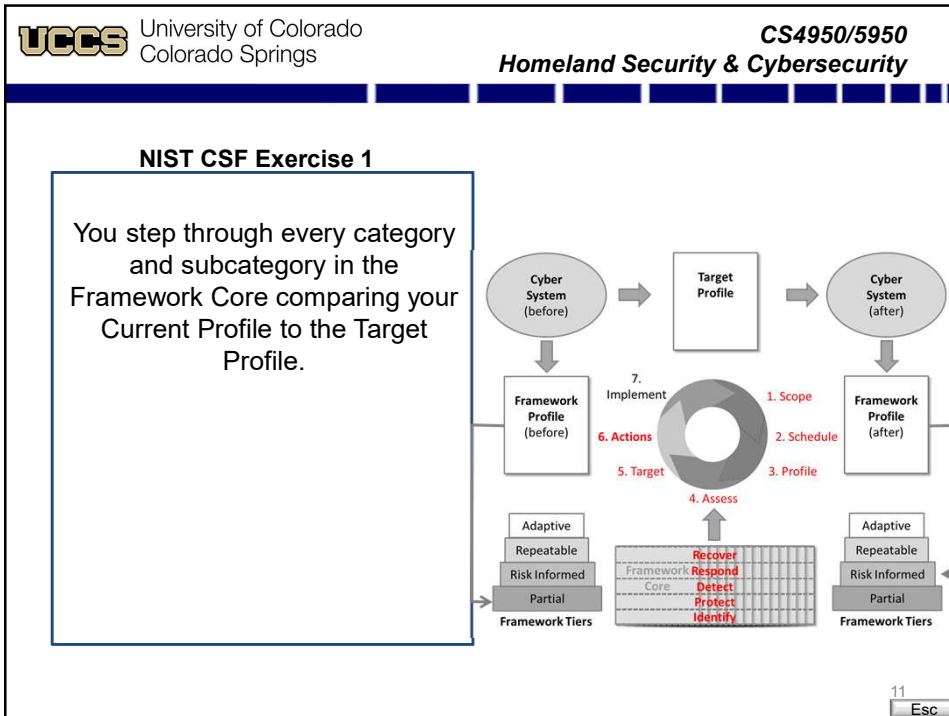
8



9



10



11

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST CSF Exercise 1

- You note that under the Access Control category you pretty much comply with subcategories 1, 2, and 3.
- That is to say, user names and passwords are required for the computer control system;
- the computer control system is kept in a locked strong room, to which only system administrators have the lock code; and
- the system is configured to prevent any unauthorized access over the Internet.

February 12, 2014 Cybersecurity Framework Version 1.0

Function	Category	Subcategory	Information References
PROTECT	Risk Management Strategy (RKM)	RKM-1: Risk management processes are established, managed, and refined to fit organizational needs.	<ul style="list-style-type: none"> NIST SP 800-60 Rev. 4 P514, P519 CORBT 9 AP011.04, AP011.05, AP011.06, B007.01, B008.02 ISA 4240-2:2009 A.1.2 NIST SP 800-60 Rev. 4 P519
		RKM-2: Organizational risk tolerance is determined and clearly expressed.	<ul style="list-style-type: none"> CORBT 9 AP011.06 ISA 4240-2:2009 A.1.2.3 NIST SP 800-60 Rev. 4 P519
		RKM-3: The organization's management of risk tolerance is aligned to its role in critical infrastructure and	<ul style="list-style-type: none"> NIST SP 800-60 Rev. 4 P514, P519, P511, 514
	Access Control (PR.AC): Access to control and associated facilities is limited to authorized users, processes, or devices and to authorized activities and transactions.	PR.AC-1: Identities and credentials are managed for authorized devices and users.	<ul style="list-style-type: none"> CIS CMC 10 CORBT 9 D0101.04, D0101.05 ISA 4240-2:2009 A.3.3.1 ISA 4240-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9 ISO/IEC 27001:2013 A.9.1.1, A.9.1.2, A.9.2.4, A.9.3.1, A.9.3.2, A.9.3.3 NIST SP 800-60 Rev. 4 AC-2, 1A Family
		PR.AC-2: Physical access to assets is managed and governed.	<ul style="list-style-type: none"> CORBT 9 D0101.04, D0101.05 ISA 4240-2:2009 A.3.3.2, A.3.3.3, B0101.2, B0101.3, B0101.4, B0101.5, B0101.6, B0101.7, B0101.8, B0101.9, B0101.10, B0101.11, B0101.12, A.11.1.6, A.11.1.7, A.11.2.3 NIST SP 800-60 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-7
		PR.AC-3: Remote access is managed.	<ul style="list-style-type: none"> CORBT 9 AP011.01, D0101.04, D0101.05 ISA 4240-2:2009 A.3.3.1 ISA 4240-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, A.11.2.1, A.11.2.2, A.11.2.3
			<ul style="list-style-type: none"> CORBT 9 AP011.01, D0101.04, D0101.05 ISA 4240-2:2009 A.3.3.1 ISA 4240-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, A.11.2.1, A.11.2.2, A.11.2.3
			<ul style="list-style-type: none"> CORBT 9 AP011.01, D0101.04, D0101.05 ISA 4240-2:2009 A.3.3.1 ISA 4240-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, A.11.2.1, A.11.2.2, A.11.2.3
			<ul style="list-style-type: none"> CORBT 9 AP011.01, D0101.04, D0101.05 ISA 4240-2:2009 A.3.3.1 ISA 4240-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, A.11.2.1, A.11.2.2, A.11.2.3

12 Esc

12



NIST CSF Exercise 1

According to your Target Profile, the next step would be to try and implement Access Control Subcategory 4, and further differentiate user access rights according to the **principles of least privilege**.

February 12, 2014 Cybersecurity Framework Version 1.0

Function	Category	Subcategory	Information References
Identify	PR.AC	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	<ul style="list-style-type: none"> NIST SP 800-63 Rev. 4 AC-17, AC-19, AC-20 CCSC SC 12.12 ISA 42440-2-2:2009 4.3.3.7.3 ISA 42440-2-2:2013 SR.2.1 ISO/IEC 27002:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 NIST SP 800-63 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-18
		PR.AC-5: Network integrity is protected, incorporating network segregation when appropriate	<ul style="list-style-type: none"> ISA 42440-2-2:2009 4.3.3.4 ISA 42440-2-2:2013 SR.3.1, SR.3.1.1 ISO/IEC 27002:2013 A.13.1.1, A.13.1.3, A.13.1.7 NIST SP 800-63 Rev. 4 AC-4, AC-7
		PR.AC-6: All users are informed and trained	<ul style="list-style-type: none"> CCSC SC 9 CORBT F-AP007 (S), BA001 (S) ISA 42440-2-2:2009 4.3.2.4.2 ISO/IEC 27002:2013 A.7.2.2 NIST SP 800-63 Rev. 4 A.7.2, PR.13
		PR.AC-7: Privileged users understand roles & responsibilities	<ul style="list-style-type: none"> CCSC SC 9 CORBT F-AP007 (S), DS006 (S) ISA 42440-2-2:2009 4.3.2.4.2, 4.3.2.4.3 ISO/IEC 27002:2013 A.6.1.1, A.7.2.2 NIST SP 800-63 Rev. 4 A.7.2, PR.13
Assess and Test	PR.AT	PR.AT-3: Third-party individuals (e.g., suppliers, contractors, partners) understand roles & responsibilities	<ul style="list-style-type: none"> CCSC SC 9 CORBT F-AP007 (S), AP003 (S), AP005 (S) ISA 42440-2-2:2009 4.3.2.4.2 ISO/IEC 27002:2013 A.6.1.1, A.7.2.2 NIST SP 800-63 Rev. 4 PS-7, SA-9
		PR.AT-4: Senior executives understand roles & responsibilities	<ul style="list-style-type: none"> CCSC SC 9 CORBT F-AP007 (S)
		PR.AT-5: All users are informed and trained	<ul style="list-style-type: none"> CCSC SC 9 CORBT F-AP007 (S), BA001 (S) ISA 42440-2-2:2009 4.3.2.4.2 ISO/IEC 27002:2013 A.7.2.2 NIST SP 800-63 Rev. 4 A.7.2, PR.13
		PR.AT-6: Privileged users understand roles & responsibilities	<ul style="list-style-type: none"> CCSC SC 9 CORBT F-AP007 (S), DS006 (S) ISA 42440-2-2:2009 4.3.2.4.2, 4.3.2.4.3 ISO/IEC 27002:2013 A.6.1.1, A.7.2.2 NIST SP 800-63 Rev. 4 A.7.2, PR.13

13

Esc

13



NIST CSF Exercise 1

- At present, all 35 utility employees have system accounts.
- With the exception of the three system administrators, all accounts have the same non-administrative access rights.

February 12, 2014 Cybersecurity Framework Version 1.0

Function	Category	Subcategory	Information References
Identify	PR.AC	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	<ul style="list-style-type: none"> NIST SP 800-63 Rev. 4 AC-17, AC-19, AC-20 CCSC SC 12.12 ISA 42440-2-2:2009 4.3.3.7.3 ISA 42440-2-2:2013 SR.2.1 ISO/IEC 27002:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 NIST SP 800-63 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-18
		PR.AC-5: Network integrity is protected, incorporating network segregation when appropriate	<ul style="list-style-type: none"> ISA 42440-2-2:2009 4.3.3.4 ISA 42440-2-2:2013 SR.3.1, SR.3.1.1 ISO/IEC 27002:2013 A.13.1.1, A.13.1.3, A.13.1.7 NIST SP 800-63 Rev. 4 AC-4, AC-7
		PR.AC-6: All users are informed and trained	<ul style="list-style-type: none"> CCSC SC 9 CORBT F-AP007 (S), BA001 (S) ISA 42440-2-2:2009 4.3.2.4.2 ISO/IEC 27002:2013 A.7.2.2 NIST SP 800-63 Rev. 4 A.7.2, PR.13
		PR.AC-7: Privileged users understand roles & responsibilities	<ul style="list-style-type: none"> CCSC SC 9 CORBT F-AP007 (S), DS006 (S) ISA 42440-2-2:2009 4.3.2.4.2, 4.3.2.4.3 ISO/IEC 27002:2013 A.6.1.1, A.7.2.2 NIST SP 800-63 Rev. 4 A.7.2, PR.13
Assess and Test	PR.AT	PR.AT-3: Third-party individuals (e.g., suppliers, contractors, partners) understand roles & responsibilities	<ul style="list-style-type: none"> CCSC SC 9 CORBT F-AP007 (S), AP003 (S), AP005 (S) ISA 42440-2-2:2009 4.3.2.4.2 ISO/IEC 27002:2013 A.6.1.1, A.7.2.2 NIST SP 800-63 Rev. 4 PS-7, SA-9
		PR.AT-4: Senior executives understand roles & responsibilities	<ul style="list-style-type: none"> CCSC SC 9 CORBT F-AP007 (S)
		PR.AT-5: All users are informed and trained	<ul style="list-style-type: none"> CCSC SC 9 CORBT F-AP007 (S), BA001 (S) ISA 42440-2-2:2009 4.3.2.4.2 ISO/IEC 27002:2013 A.7.2.2 NIST SP 800-63 Rev. 4 A.7.2, PR.13
		PR.AT-6: Privileged users understand roles & responsibilities	<ul style="list-style-type: none"> CCSC SC 9 CORBT F-AP007 (S), DS006 (S) ISA 42440-2-2:2009 4.3.2.4.2, 4.3.2.4.3 ISO/IEC 27002:2013 A.6.1.1, A.7.2.2 NIST SP 800-63 Rev. 4 A.7.2, PR.13

14

Esc

14



NIST CSF Exercise 1

- Now let's set it aside and take a look at the Awareness and Training category, and notice that we have implemented none of its subcategories.
- All 35 employees were granted a system account without undergoing any kind of internal training.**

February 12, 2014 Cybersecurity Framework Version 1.0

Function	Category	Subcategory	Information References
			<ul style="list-style-type: none"> NIST SP 800-63 Rev. 4 AC-1, AC-1F, AC-2 CCSC SC-1 ISA 62443-3-2:2009 A.3.3.3 ISA 62443-3-2:2009 A.3.3.1 ISO/IEC 27001:2013 A.5.1.2, A.5.1.3, A.5.1.4 NIST SP 800-63 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-7
		PR.AC-4: Access permissions are managed, incorporating the principle of least privilege and separation of duties.	<ul style="list-style-type: none"> ISA 62443-3-2:2009 A.3.3.4 ISA 62443-3-2:2009 A.3.3.1, A.3.3.2, A.3.3.3 ISO/IEC 27001:2013 A.5.1.1, A.5.1.2, A.5.1.3 NIST SP 800-63 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-7
		PR.AC-5: Network security is protected, incorporating network segmentation where appropriate.	<ul style="list-style-type: none"> ISA 62443-3-2:2009 A.3.3.4 ISA 62443-3-2:2009 A.3.3.1, A.3.3.2, A.3.3.3 ISO/IEC 27001:2013 A.5.1.1, A.5.1.2, A.5.1.3 NIST SP 800-63 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-7
	Awareness and Training (PR.AT)	PR.AT-1: All users are informed and trained.	<ul style="list-style-type: none"> CCSC SC-2 COBET 4 APOUT-01, BA001-01 ISA 62443-3-2:2009 A.3.3.2, A.3.3.3 ISO/IEC 27001:2013 A.7.2.2 NIST SP 800-63 Rev. 4 AT-2, PM-1.1
		PR.AT-2: Privileged users understand roles & responsibilities.	<ul style="list-style-type: none"> CCSC SC-3 COBET 4 APOUT-02, D0008-03 ISA 62443-3-2:2009 A.3.3.2, A.3.3.3 ISO/IEC 27001:2013 A.7.2.2, A.7.2.3 NIST SP 800-63 Rev. 4 AT-2, PM-1.1
		PR.AT-3: Third-party relationships (e.g., suppliers, contractors, partners) understand roles & responsibilities.	<ul style="list-style-type: none"> CCSC SC-4 COBET 4 APOUT-03, APO010-04, APO010-05 ISA 62443-3-2:2009 A.3.3.2, A.3.3.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-63 Rev. 4 AT-2, PM-1.1
		PR.AT-4: Senior executives understand roles & responsibilities.	<ul style="list-style-type: none"> CCSC SC-5 COBET 4 APOUT-04

15

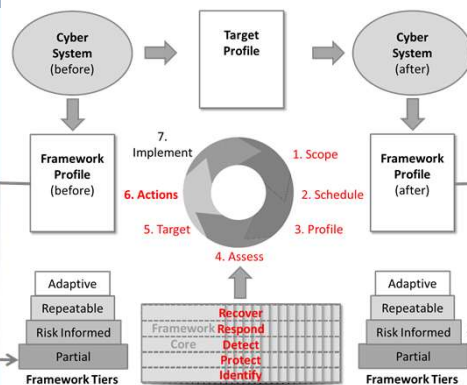
Esc

15



NIST CSF Exercise 1

Question: Do you think implementing Access Control Subcategory 4, further differentiating access rights based on the principle of least privilege is more important, or do you think that creating a training program before granting system access, according to Awareness and Training Subcategory 1 is more important?



16

Esc

16

UCCS University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST CSF Exercise 1

- The correct answer is **there is no correct answer**, even if some of you said both should have the same priority.
- A strong argument can be made to give either measure precedence over the other.

17 Esc

17

UCCS University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST CSF Exercise 1

- The one you choose depends upon a lot of factors, not the least of which is your own knowledge and experience.
- This is perfectly legitimate.
- The point is you've identified the gaps and you can reasonably assess the risk of each.**

18 Esc

18

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST CSF Exercise 1

- You have advanced your organization from ignorance to understanding.**
- You can now craft a risk based strategy for implementing whichever measure you chose first, and aware of the latent risk doing the other second.

19 Esc

19

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

NIST CSF Exercise 1

The point of this exercise was to provide you some insight into the actual application of the NIST Cybersecurity Framework, and some appreciation for the challenges attendant to the task.

20 Esc


20

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Conclusion

Questions?



21

Esc