

University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**


---

**ES-C2M2 Exercise 3**

CS 4950/5950  
Homeland Security &  
Cybersecurity

**Lesson 21**  
**ES-C2M2**  
**Exercise 3**


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



1

Esc

1



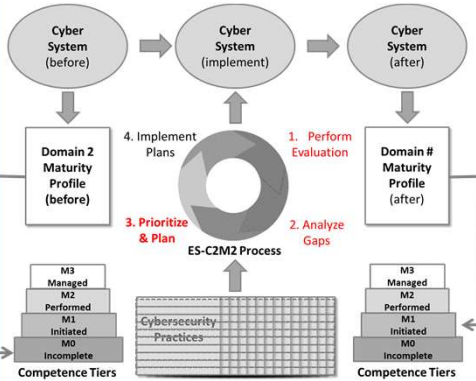
University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

**ES-C2M2 Exercise 3**

- Step 3 in the ES-C2M2 Process is "Prioritize and Plan".
- The idea behind this step is that you may not have enough funds necessary in this budget cycle to implement all the Domain Objectives necessary to achieve your target Maturity Levels.
- Accordingly, whenever faced with more tasks than resources, you must prioritize.
- But how do you prioritize?**



2

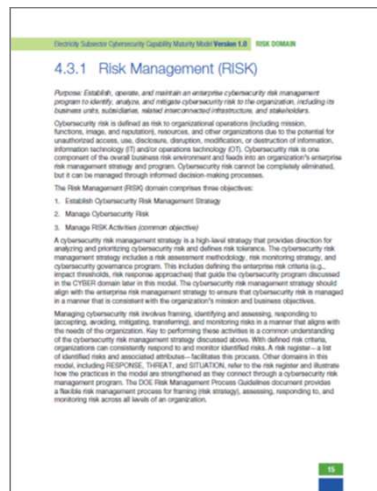
Esc

2



## ES-C2M2 Exercise 3

- Domain 1 of the ES-C2M2 Cybersecurity Practices advocates a risk management approach, but it doesn't specify any particular risk methodology.
- There are certainly many out there to choose from, at least 250 by one estimate.
- I personally have only seen about 40.



3

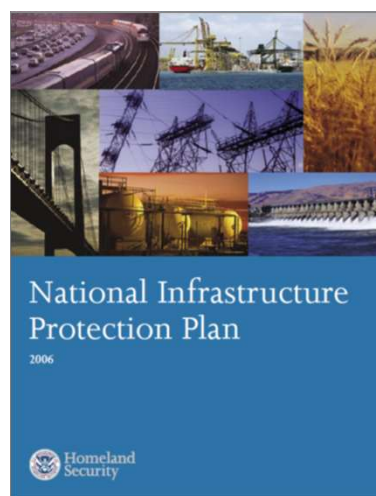
Esc

3



## ES-C2M2 Exercise 3


In 2006, the first National Infrastructure Protection Plan advocated a risk methodology called **RAMCAP**, the Risk Analysis and Management for Critical Asset Protection.



4

Esc

4



University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

**ES-C2M2 Exercise 3**

- RAMCAP was developed by the American Society of Mechanical Engineers at the request of the White House shortly following 9/11.
- RAMCAP assesses risk as the product of threat, vulnerability, and consequence.
- **$R = T \times V \times C$**


**RAMCAP**  
**Risk Assessment**

Risk Analysis and Management for  
Critical Asset Protection


**$R = T \times V \times C$**

- R = Risk
- T = Threat
- V = Vulnerability
- C = Consequence

5



5



University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

**ES-C2M2 Exercise 3**


- RAMCAP uses this risk estimate to calculate Return on Investment and perform Cost-Benefit Analysis.
- RAMCAP calculates the Return on Investment by dividing the estimated risk a given countermeasure by its estimated cost.
- **$ROI = R / \$$**

**RAMCAP**  
**Return on Investment**


$ROI = R / \$$

- R = RAMCAP Risk
- \$ = Countermeasure Cost

6



6



University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

**ES-C2M2 Exercise 3**

- RAMCAP performs cost-benefit analysis by giving highest priority to the countermeasure offering the highest return on investment.
- Unfortunately, **RAMCAP is a very involved process**, which probably contributed to its rapid disappearance shortly after it was introduced in 2006.


**RAMCAP**  
**Cost Benefit Analysis**

- If  $ROI1 > ROI2$  then ROI1
- If  $ROI2 > ROI1$  then ROI2
- If  $ROI1 = ROI2$  then "tossup"

7

Esc

7



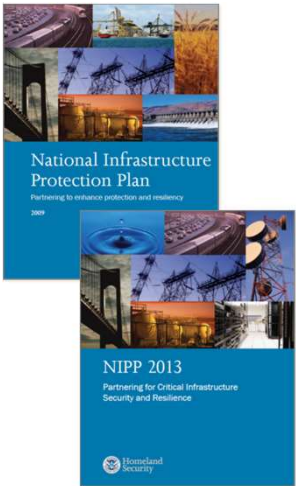
University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

**ES-C2M2 Exercise 3**


- RAMCAP was not mentioned in either the 2009 or 2013 National Infrastructure Protection Plans.
- RAMCAP's sole surviving role is as the foundation for the American Water Works Association J100-10 standard for "Risk and Resilience Management of Water and Wastewater Systems".
- **Still, it does offer a methodology, and one with a pedigree that no other methodology can match.**



8

Esc

8



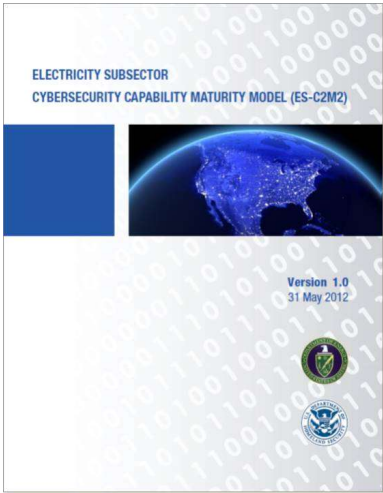
University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

**ES-C2M2 Exercise 3**


- Let's take a look at how we might apply RAMCAP to Electricity Subsector Cybersecurity Capability Maturity Model.
- First, let us consider that each Domain Objectives identified in Step 2 of the Electricity Subsector Cybersecurity Capability Maturity Model is each a countermeasure.



9

Esc

9



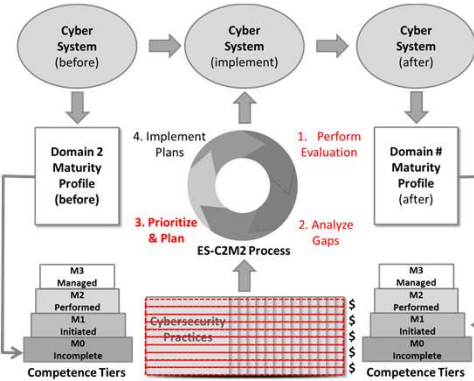
University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

**ES-C2M2 Exercise 3**


- Accordingly, we need to estimate the cost of each identified Domain Objective.
- That is not too difficult.
- We need only estimate the time and materials required to implement each Domain Objective and combine them into a single dollar cost.**



10

Esc

10



University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

**ES-C2M2 Exercise 3**


- Next, we need to estimate a risk value for each Domain Objective.
- Using RAMCAP, we will estimate risk as the product of threat, vulnerability, and consequence.
- $R = T \times V \times C$
- **First, we will need to estimate the value of each term before multiplying them together.**

**RAMCAP**  
**Risk Assessment**


Risk Analysis and Management for  
Critical Asset Protection

**$R = T \times V \times C$**

- R = Risk
- T = Threat
- V = Vulnerability
- C = Consequence

11  


11




University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**


---

**ES-C2M2 Exercise 3**

- RAMCAP estimates the **Worst Reasonable Consequence** that might result from a specific component failure.
- We will do the same by estimating the Worst Reasonable Consequence of not implementing each identified Domain Objective.
- RAMCAP derives a consequence value by extrapolating the estimated losses due to deaths and damages from a finite exponential scale.
- We don't need to be nearly so elaborate.

12  


12



University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

**ES-C2M2 Exercise 3**

For simplicity, we will **assign a consequence value 1, 2, or 3** based on our estimation of whether the failure to implement a specific Domain Objective could result in low, medium, or high losses to the electric utility.


**RAMCAP**  
**Consequence Estimation**

- C = 1 = low consequence
- C = 2 = med consequence
- C = 3 = high consequence

13

Esc

13



University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

**ES-C2M2 Exercise 3**

- Now let us estimate a value for the “vulnerability” term.
- For “vulnerability” we will assign a value of “1” because we know that we are 100% vulnerable to the absence of each identified Domain Objective.**
- Makes sense, right?


**RAMCAP**  
**Vulnerability Estimation**

- V = Likelihood system will succumb to this vulnerability
- V = 1
- 100% vulnerable to threats associated with given Domain Objective because it has not yet been implemented

14

Esc

14



University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**


---

**ES-C2M2 Exercise 3**


- Finally, let us estimate a value for the **threat term**, representing the likelihood this particular vulnerability will be exploited.
- Again, for simplicity sake, we will **assign a threat value of 0.0001, 0.001, or 0.01** based on our estimation that the absence of this particular Domain Objective will likely be exploited is low, medium, or high.

**RAMCAP**  
**Threat Estimation**

- T = Likelihood that this particular vulnerability will be exploited
- T = 0.0001 = low likelihood
- T = 0.001 = med likelihood
- T = 0.01 = high likelihood

15  


15



University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---


**ES-C2M2 Exercise 3**

Using these data values will result in calculated risks ranging from 0.0001% to 3% when we multiply the threat, vulnerability, and consequence values.

**RAMCAP**  
**Risk Analysis**


**$R = T \times V \times C$**

R	T	V	C	
0.0001	0.0001	1	1	low
0.002	0.001	1	2	med
0.03	0.01	1	3	high

16  


16





University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

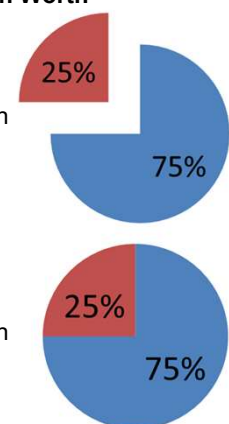
**ES-C2M2 Exercise 3**

- Now remember, this is the risk from not implementing a given Domain Objective, which means **we can expect an equivalent amount of risk reduction by implementing the given Domain Objective.**
- In other words, the higher the risk, the greater the reward by eliminating it.

**Risk Reduction Worth**

Amount of risk Assumed by **not implementing** given Domain Objective.


Amount of risk Reduction by **implementing** given Domain Objective.



17

Esc

17



University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

**ES-C2M2 Exercise 3**

- Therefore, we may consider the calculated risk for each Domain Objective as its equivalent “risk reduction worth”.
- We are now closer to assigning priorities.

**RAMCAP**  
**Risk Reduction Worth**


$R = T \times V \times C$

R = Risk = Risk Reduction Worth

18

Esc

18



University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

**ES-C2M2 Exercise 3**

For each identified Domain Objective necessary to achieve our next Maturity Level we now have two pieces of important information:


- 1) the estimated cost of implementation, and**
- 2) its estimated risk reduction worth.**

We now calculate the RAMCAP return on investment for each Domain Objective.


**RAMCAP**  
**Risk Management**

**For each domain objective:**

1. Estimated cost to implement
2. Estimated risk reduction worth

19  


19



University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**


---

**ES-C2M2 Exercise 3**


- So, let's say we have two different Domain Objectives, DO1 and DO2, and have estimated their respective implementation costs at \$10 and \$100 respectively.
- By the same token, we have conducted RAMCAP risk analysis on each Domain Objective and estimated both their risks at 3%
- Which Domain Objective gives us the highest return on investment?**

**RAMCAP**  
**Risk Management**

1. DO1 = \$10 to implement
2. DO2 = \$100 to implement

20  


20



University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

**ES-C2M2 Exercise 3**


- We calculate the Return on Investment by dividing the estimated risk by the estimated cost.
- $ROI = R / \$$

**RAMCAP**  
**Risk Management**


1. D01 = \$10 to implement  
R = 3%
2. D02 = \$100 to implement  
R = 3%

**Which Domain Objective gives the highest return on investment?**

21



21



University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

**ES-C2M2 Exercise 3**


In the case of our example, the calculated return on investment is 0.003 for DO1, and 0.0003 for DO2.

**RAMCAP**  
**Return on Investment**


$ROI1 = R1 / \$$   
 $ROI2 = R2 / \$$

	Estimated Cost	Estimated Risk	Calculated ROI
<b>D01</b>	\$10	3%	
<b>D02</b>	\$100	3%	

22



22



University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

**ES-C2M2 Exercise 3**

- According to RAMCAP cost-benefit analysis, the countermeasure with the highest return on investment receives the highest priority.
- In our example, DO1 has a higher return on investment than DO2, and therefore receives the highest priority.

**RAMCAP**  
**Cost Benefit Analysis**


- If ROI1 > ROI2 then ROI1
- If ROI2 > ROI1 then ROI2
- If ROI1 = ROI2 then "tossup"

	Estimated Cost	Estimated Risk	Calculated ROI
D01	\$10	3%	0.0030
D02	\$100	3%	0.0003

23

Esc

23



University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

**ES-C2M2 Exercise 3**

- Okay, so let's say this time we have Domain Objective 3 and Domain Objective 4, except this time we estimate the risk for each at 2% and 3% respectively.
- That is to say that the estimated risk reduction worth of DO3 is 2% and the risk reduction worth of DO4 is 3%


**RAMCAP**  
**Risk Management**

1. D03; R = 2%
2. D04; R = 3%

24

Esc

24



University of Colorado  
Colorado Springs

CS4950/5950  
**Homeland Security & Cybersecurity**

---

**ES-C2M2 Exercise 3**


- However, as before, DO3 is significantly cheaper than DO4.
- DO3 costs \$10 while DO4 costs \$100 to implement.
- **Which Domain Objective provides the highest return on investment?**

**RAMCAP**  
**Risk Management**


- D03 = \$10 to implement  
R = 2%
- D04 = \$100 to implement  
R = 3%

**Which Domain Objective gives the highest return on investment?**

25



25



University of Colorado  
Colorado Springs

CS4950/5950  
**Homeland Security & Cybersecurity**

---

**ES-C2M2 Exercise 3**


- The return on investment is 0.002 for DO3, but only 0.0003 for DO4.
- The return on investment is higher for Domain Objective 3 than Domain Objective 4.
- **Accordingly, DO3 receives a higher priority than DO4.**

**RAMCAP**  
**Cost Benefit Analysis**


- If ROI3 > ROI4 then ROI3
- If ROI4 > ROI3 then ROI4
- If ROI3 = ROI4 then "tossup"

	Estimated Cost	Estimated Risk	Calculated ROI
<b>D03</b>	\$10	2%	<b>0.0020</b>
<b>D04</b>	\$100	3%	<b>0.0003</b>

26



26



University of Colorado  
 Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

**ES-C2M2 Exercise 3**

- Let's say you now have Domain Objectives DO5 and DO6, with estimated cost and risk terms as shown in the table.
- Which Domain Objective offers the highest return on investment?


**RAMCAP**  
Risk Management

**Which Domain Objective gives the highest return on investment?**

	Estimated	Estimated	Estimated	Estimated	Estimated	Calculated
	Cost	T	V	C	R	ROI
<b>DO5</b>	\$20	1%	1	1		
<b>DO6</b>	\$10	1%	1	2		

27 Esc

27



University of Colorado  
 Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

**ES-C2M2 Exercise 3**

- Estimate risk using the RAMCAP method by multiplying the threat, vulnerability, and consequence terms for each Domain Objective.
- Accordingly, you estimated risk for DO5 at 1%, and the risk for DO6 and 2%, remembering that these are also the estimated risk reduction to be gained by implementing the corresponding Domain Objective.

**RAMCAP**  
Risk Analysis


$$R5 = T \times V \times C$$

$$R6 = T \times V \times C$$

	Estimated	Estimated	Estimated	Estimated	Estimated	Calculated
	Cost	T	V	C	R	ROI
<b>DO5</b>	\$20	1%	1	1	1%	
<b>DO6</b>	\$10	1%	1	2	2%	

28 Esc

28



University of Colorado  
 Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---


**ES-C2M2 Exercise 3**

- Once you have estimated risk, you divide it by the corresponding estimated cost for each Domain Objective.
- So for DO5, you divide 1% by \$20, and for DO6 you divide 2% by \$10.


**RAMCAP**  
**Return on Investment**

ROI5 = R5 / \$  
ROI6 = R6 / \$

	Estimated Cost	Estimated T	Estimated V	Estimated C	Estimated R	Calculated ROI
<b>DO5</b>	\$20	1%	1	1	1%	0.0005
<b>DO6</b>	\$10	1%	1	2	2%	0.0020

29 

29



University of Colorado  
 Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---


**ES-C2M2 Exercise 3**

- The results indicate that you receive a 0.0005 return on investment for DO5, but a 0.002 return on investment for DO6.
- Accordingly, DO6 offers the higher return on investment.**


**RAMCAP**  
**Return on Investment**

If ROI5 > ROI6 then ROI5  
 If ROI6 > ROI5 then ROI6  
 If ROI5 = ROI6 then "tossup"

	Estimated Cost	Estimated T	Estimated V	Estimated C	Estimated R	Calculated ROI
<b>DO5</b>	\$20	1%	1	1	1%	0.0005
<b>DO6</b>	\$10	1%	1	2	2%	0.0020

30 

30



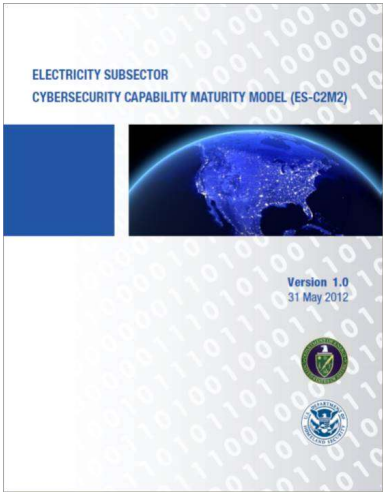
University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---


**ES-C2M2 Exercise 3**

So now you have an objective  
method for prioritizing  
implementation actions!



31  
Esc

31




University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

**Conclusion**

Questions?



32  
Esc

32