University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001/27002

CS 4950/5950
Homeland Security & Cybersecurity

Lesson 24
Exercise 3

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

1
Esc

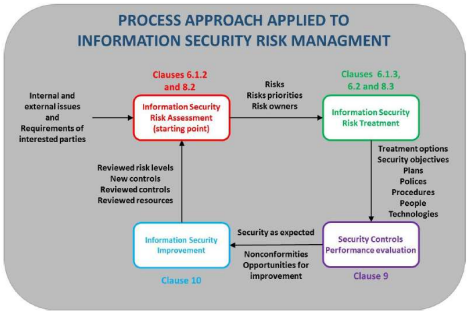
1

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 3

- This will be our final look at ISO 27001 ISMS.
- **ISO 27001 Step 2 develops and implements a Risk Treatment Plan to mitigate identified risks.**
- Let's see if you can mitigate cyber risks by answering some questions about the abstracted Internet model I have displayed.



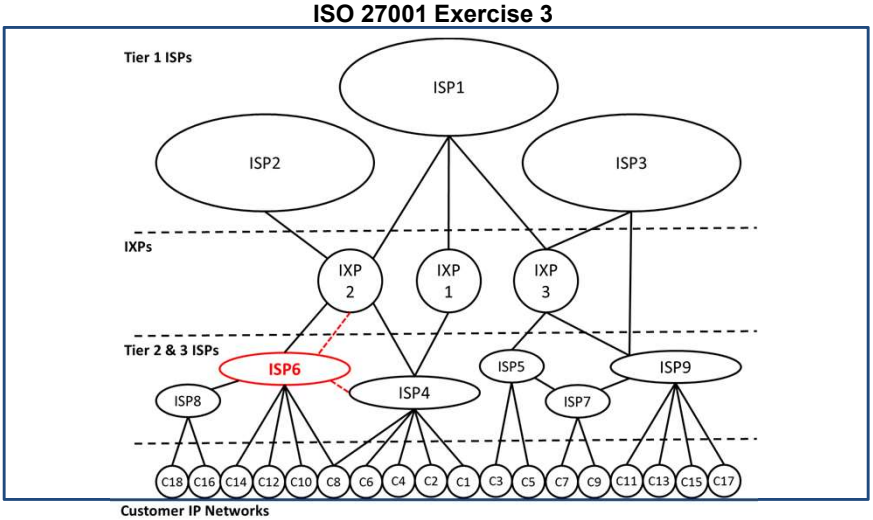
2
Esc

2

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 3



Q1: What is best way for ISP6 to reduce risk, add an extra link to IXP2 or ISP4?

3

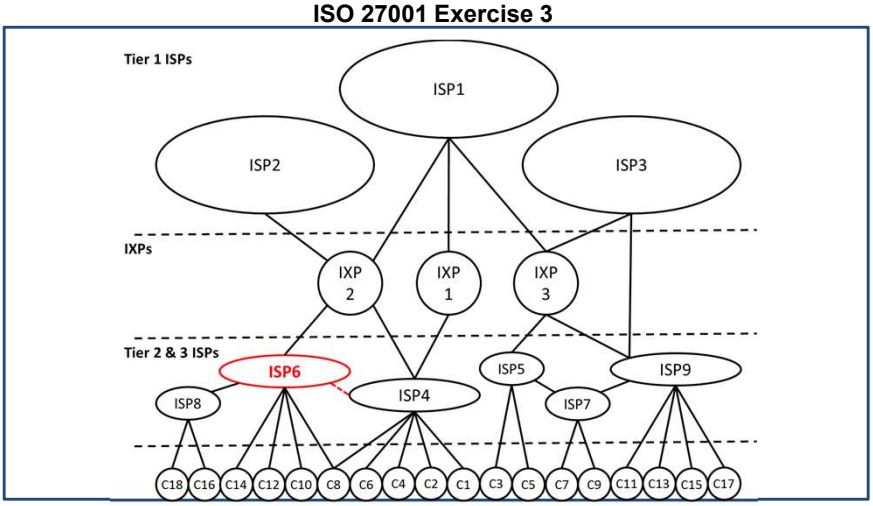
Esc

3

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 3



Q1: What is best way for ISP6 to reduce risk, add an extra link to IXP2 or ISP4?
A1: Add link to ISP4.

4

Esc

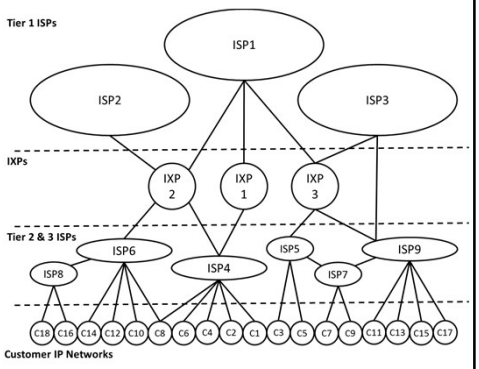
4

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 3

- Establishing a new link to ISP4 would be the better choice for adding a redundant external link.
- **While IXPs are very reliable, a failure on the IXP2 main router would render both ISP6 links useless.**
- Adding a second link to IXP2 would be creating a single point of failure in your network.



5

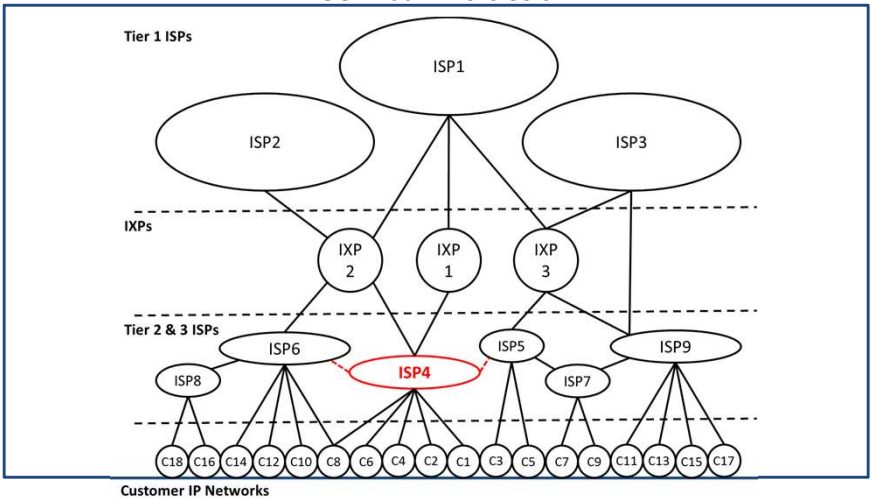
Esc

5

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 3



Q2: What is best way for ISP4 to add redundancy, add a link to ISP6 or ISP5?

6

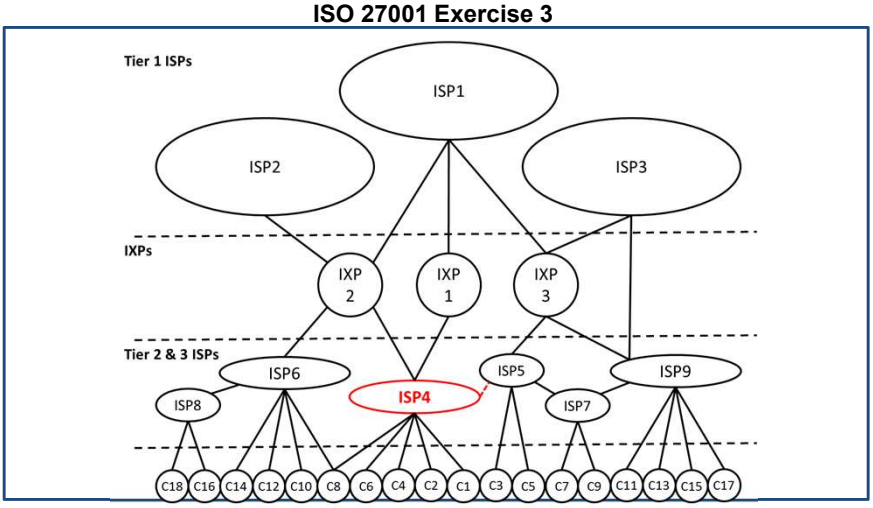
Esc

6

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 3



Q2: What is best way for ISP4 to add redundancy, add a link to ISP6 or ISP5?
A2: Add link to ISP5.

7

Esc

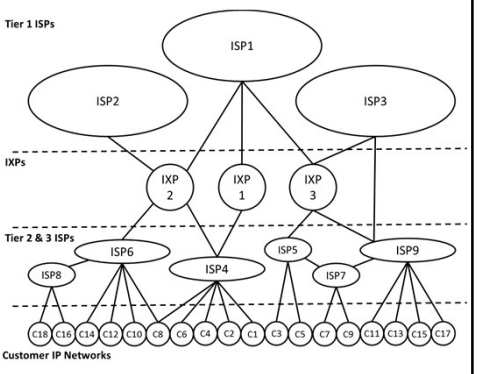
7

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 3

- ISP5 offers a better return on investment because it opens a shorter route from the "even" to "odd" side of the network.
- **We see in this question that speed and efficiency are also important determining factors in addition to reliability.**



8

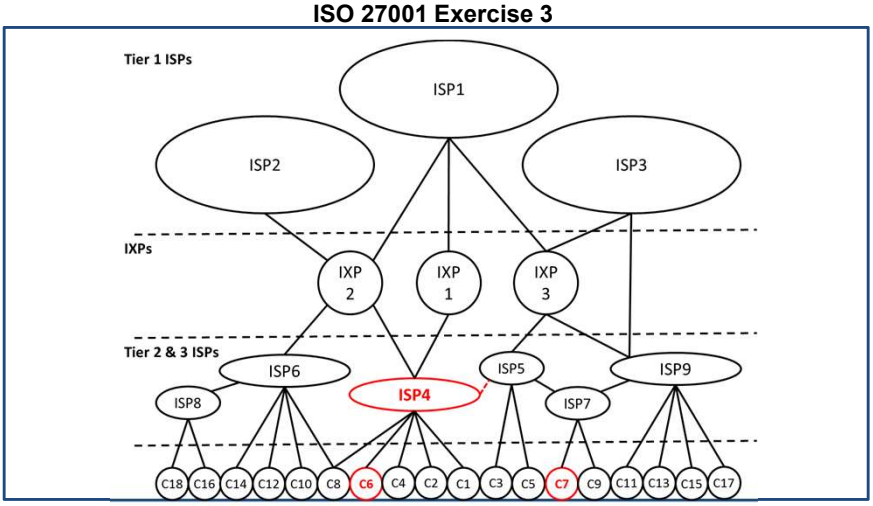
Esc

8

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 3



Q3: New link from ISP4 to ISP5 saves how many hops going from C6 to C7?

9

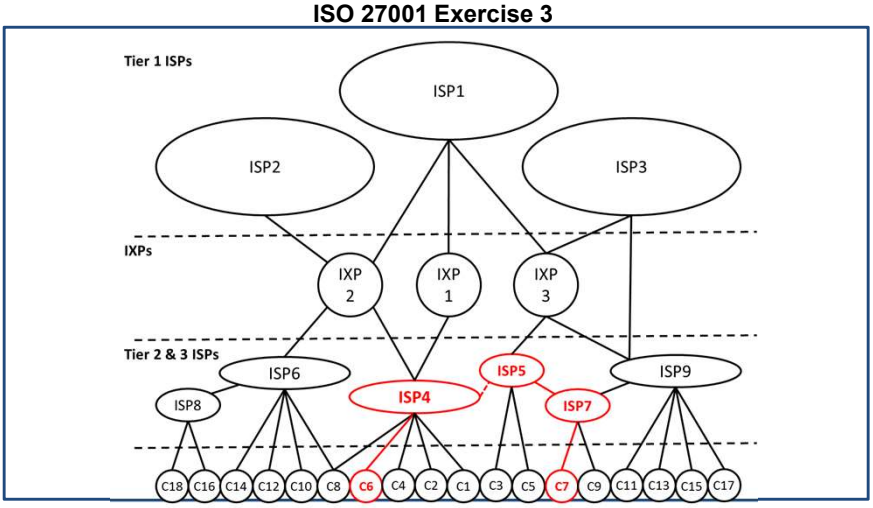
Esc

9

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 3



Q3: New link from ISP4 to ISP5 saves how many hops going from C6 to C7?
A3: Three

10

Esc

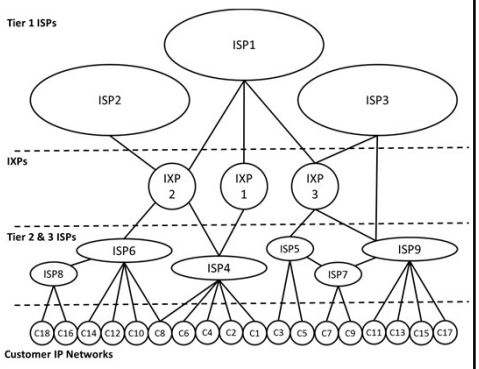
10

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 3

- Count the number of hops it takes to move a packet from C6 to C7 before the new link is installed... It takes 7 hops.
- Next, count the number of hops it would take to move a packet from C6 to C7 after the new link is installed... 4 hops.
- The difference between the two paths is 7 hops minus 4 hops equals 3 hops.



11

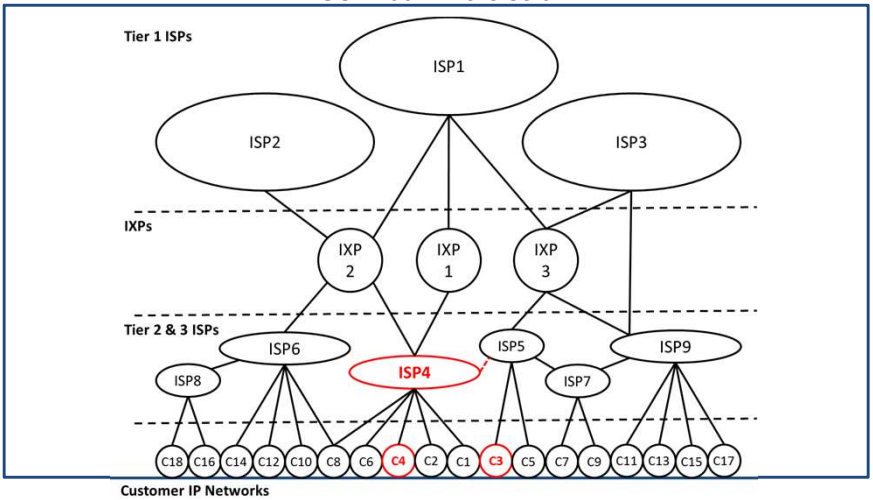
Esc

11

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 3



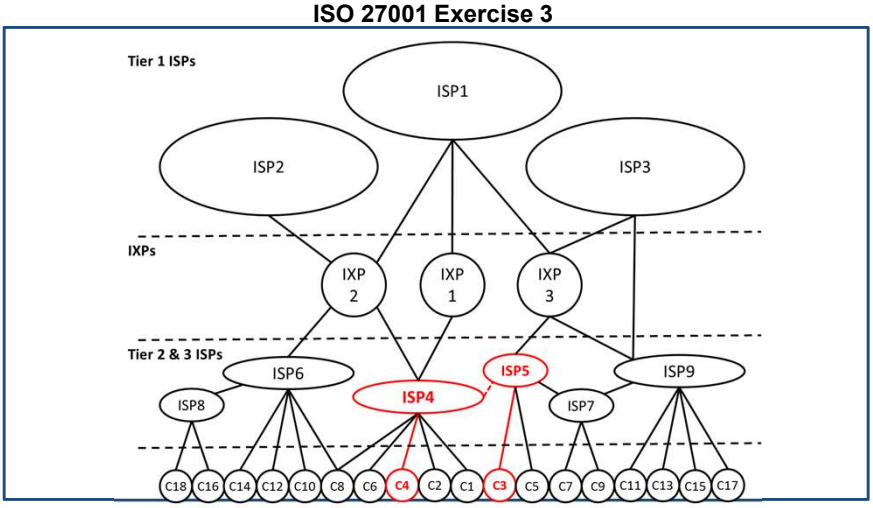
Q4: New link from ISP4 to ISP5 saves how many hops going from C3 to C4?

12

Esc

12

ISO 27001 Exercise 3

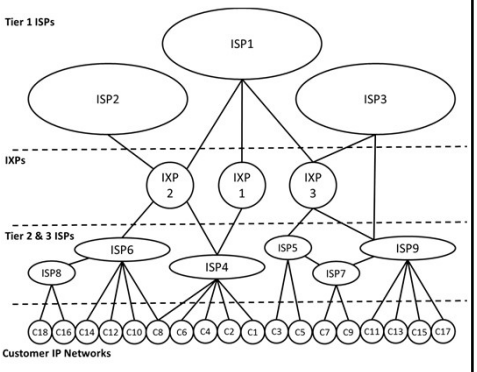


Q4: New link from ISP4 to ISP5 saves how many hops going from C3 to C4?
A4: Three

University of Colorado Colorado Springs
CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 3

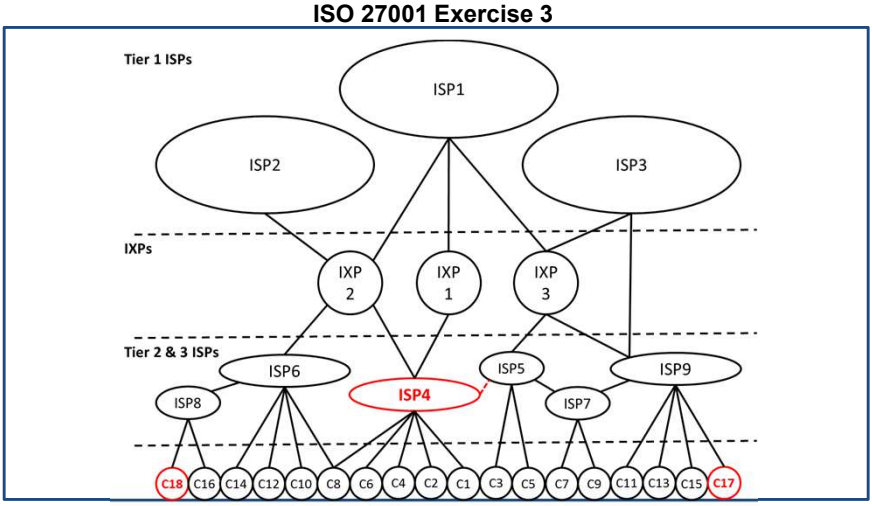
- Same method as before...
- At present, it takes 6 hops to send a data packet from C3 to C4.
- Install the new link and takes only 3 hops to send a data packet from C3 to C4.
- The difference between the two paths is 6 hops minus 3 hops equals 3 hops.



University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 3



Q5: New link from ISP4 to ISP5 saves how many hops going from C17 to C18?

15

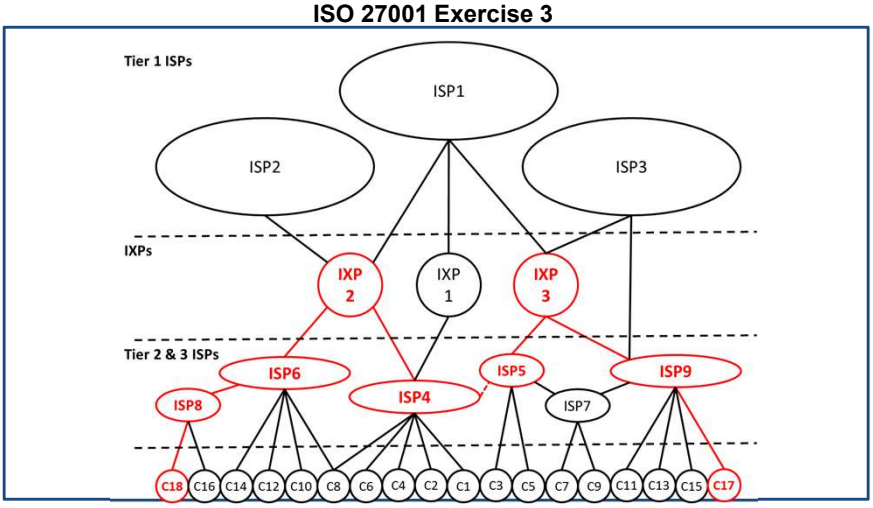
Esc

15

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 3



Q5: New link from ISP4 to ISP5 saves how many hops going from C17 to C18?
A5: Zero

16

Esc

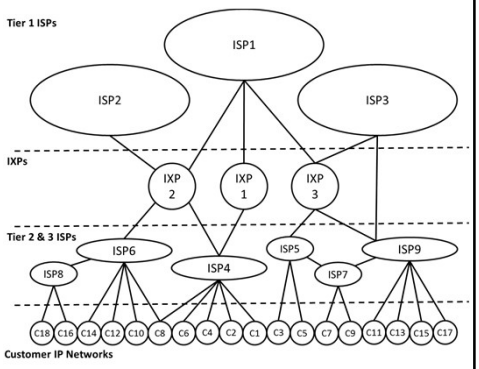
16

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 3

- Installing a new link between ISP4 and ISP5 doesn't shorten the path between C17 and C18.
- In fact, if forced to travel between ISP4 and ISP5, a data packet going from C17 to C18 would have to make at least one more hop than it otherwise would.
- **In this case installing the new link increases reliability but doesn't necessarily improve efficiency.**
- Yeah, trick question. Not really.



17

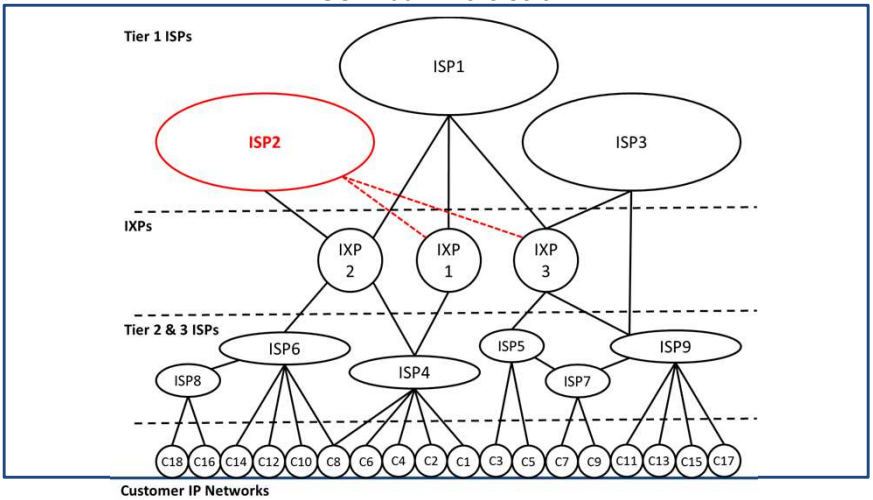
Esc

17

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 3



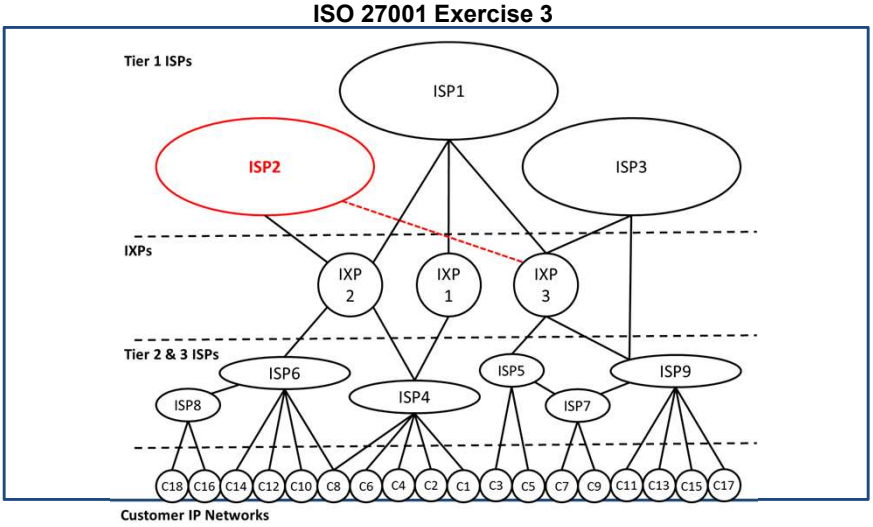
Q6: What is best way for ISP2 to add redundancy, add a link to IX1 or IXP3?

18

Esc

18

ISO 27001 Exercise 3

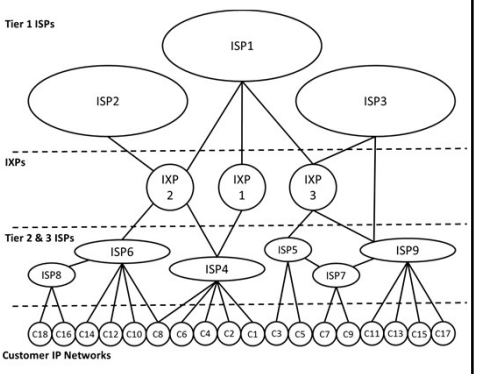


Q6: What is best way for ISP2 to add redundancy, add a link to IX1 or IXP3?
A6: Add link to IXP3.

19

ISO 27001 Exercise 3

- Connecting to IXP3 offers the better return on investment because it provides a bridge reducing the number of hops to send data packets between the "even" and "odd" sides of the network.
- **Yes, connecting to IXP3 not only increases reliability, it also improves efficiency.**

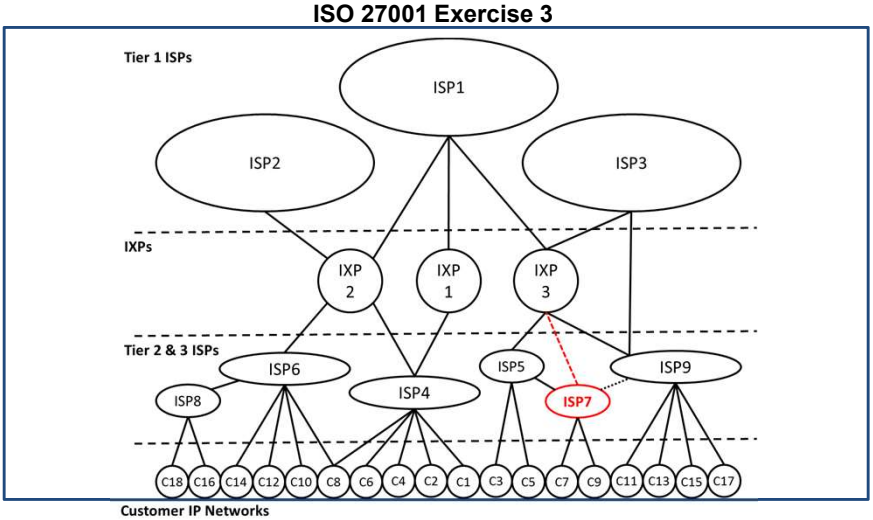


20

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 3



Q7: Should ISP7 switch its link from ISP9 to IXP3, yes or no?

21

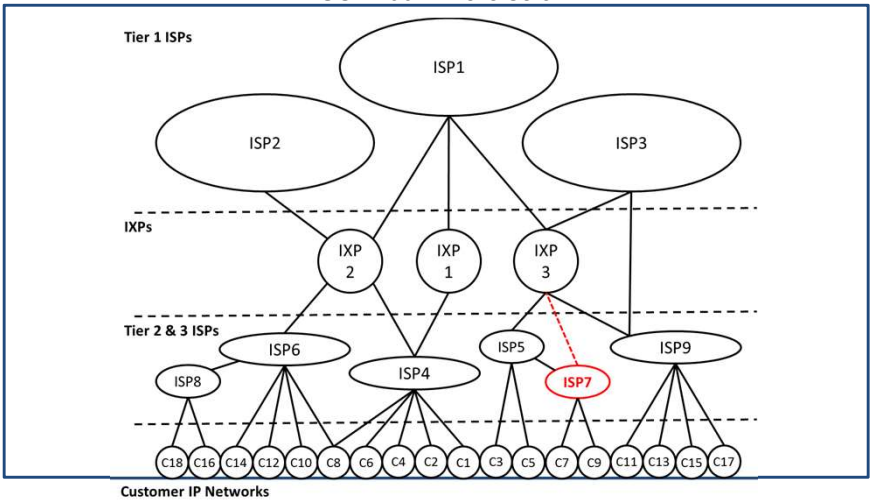
Esc

21

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 3



Q7: Should ISP7 switch its link from ISP9 to IXP3, yes or no?
A7: Yes

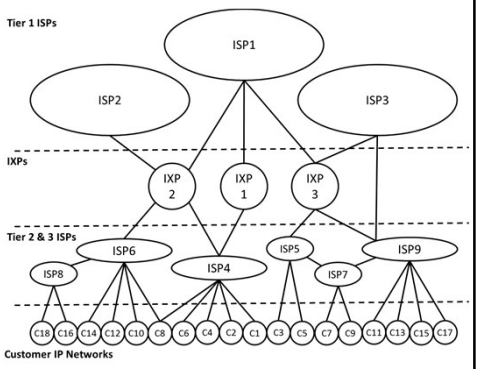
22

Esc

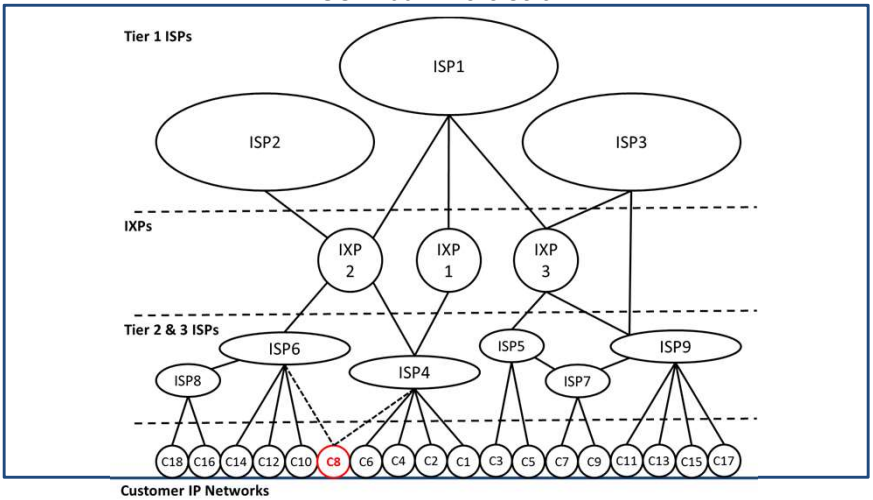
22

ISO 27001 Exercise 3

- So long as ISP7 can afford it, they are buying greater capacity in addition to redundancy.
- **IXPs are faster than ISPs. Again, this is an efficiency bonus.**



ISO 27001 Exercise 3

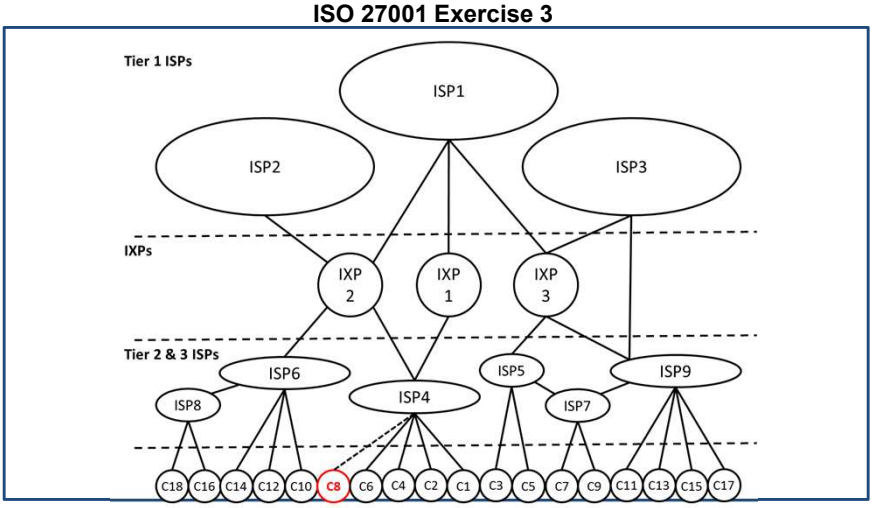


Q8: Should C8 cut its link to ISP4 or ISP6?

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 3



Q8: Should C8 cut its link to ISP4 or ISP6?
A8: Cut link to ISP6.

25

Esc

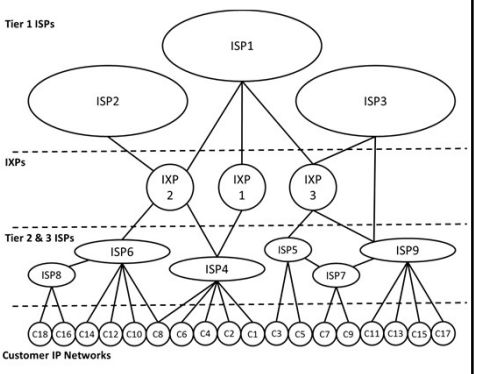
25

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 3

Keeping ISP4 is the better choice because it has a redundant link extending to an extra IXP, giving it better reliability.



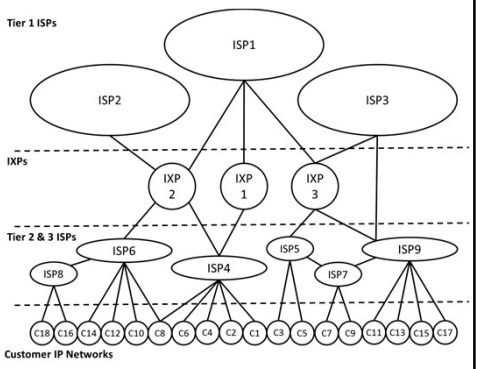
26

Esc

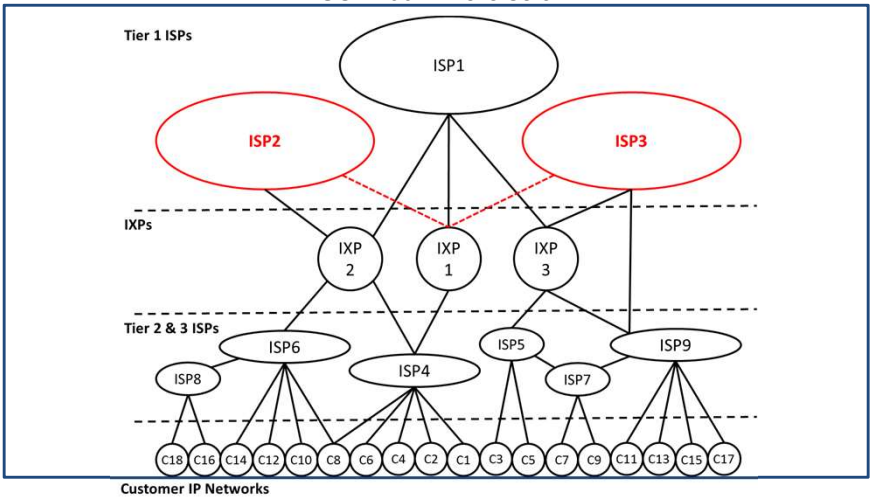
26

ISO 27001 Exercise 3

- Problem is, as a customer, you would probably never know this.
- And so far as you know from past experience, both links are equally reliable.
- **So while ISP4 would probably offer the better return on investment, you would have to dig deep into the ISPs capability to find this information.**



ISO 27001 Exercise 3

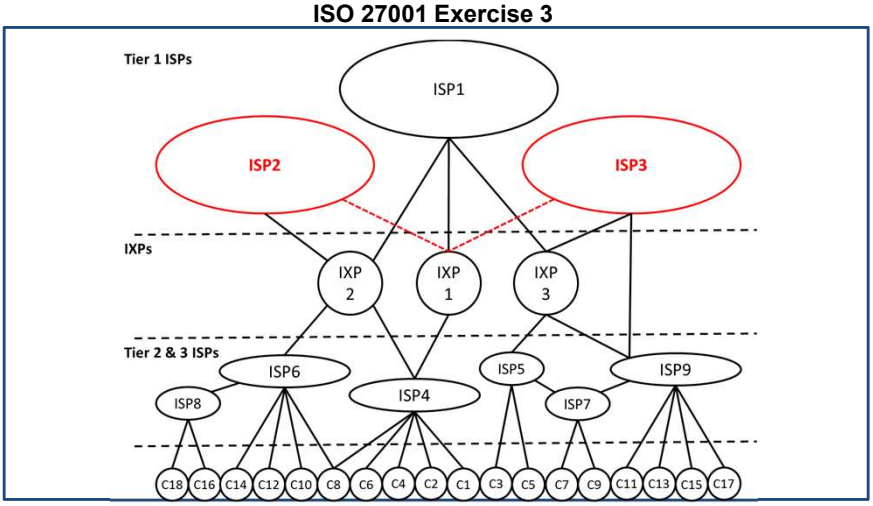


Q9: Which would benefit more by adding a link to IXP1, ISP2 or ISP3?

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 3



Q9: Which would benefit more by adding a link to IXP1, ISP2 or ISP3?
A9: ISP3

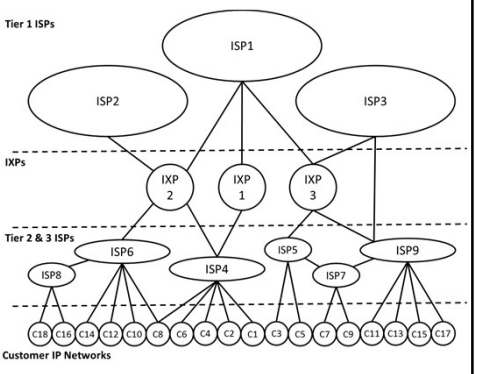
29
Esc

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 3

- **ISP3 will benefit more than ISP2 because not only will ISP3 increase redundancy, ISP3 will also gain a bridge between the "odd" and "even" sides of the network.**
- Again, ISP3 improves both reliability and efficiency.
- ISP2 gains no equivalent benefit.

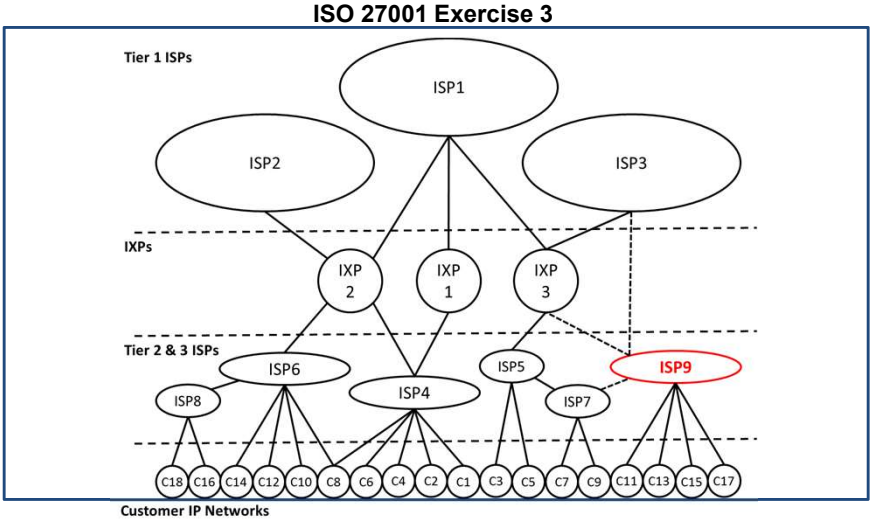


30
Esc

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 3



Q10: Which link should ISP9 cut to save money, ISP7, IXP3, or ISP3?

31

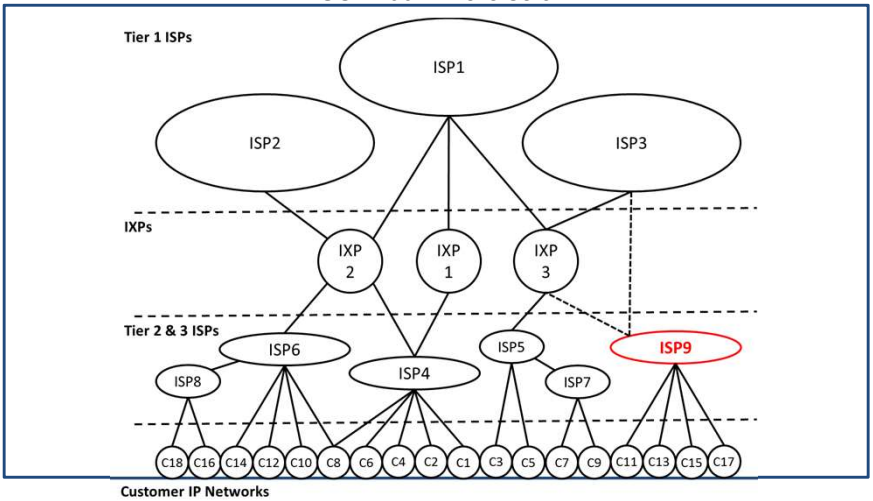
Esc

31

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 3



Q10: Which link should ISP9 cut to save money, ISP7, IXP3, or ISP3?
A10: Cut link to ISP7.

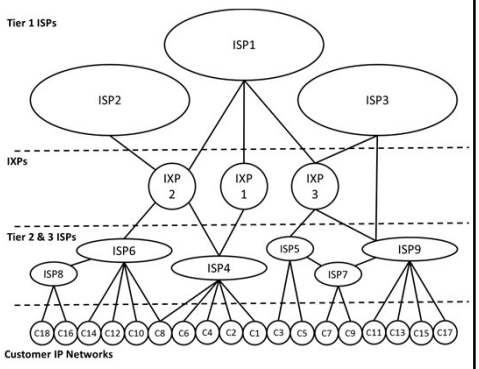
32

Esc

32

ISO 27001 Exercise 3

- Cutting the link to ISP7 would be the better choice.
- **All else being equal, cutting the link from ISP9 to ISP7 would be most prudent as IXP1 and ISP3 are capable of accepting a higher volume of traffic compared to ISP7.**
- Cutting the link to ISP7 reduces ISP9's traffic capacity by the least amount.



Conclusion

Questions?