University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001/27002

CS 4950/5950
Homeland Security & Cybersecurity

Lesson 24
Exercise 2

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

1
Esc

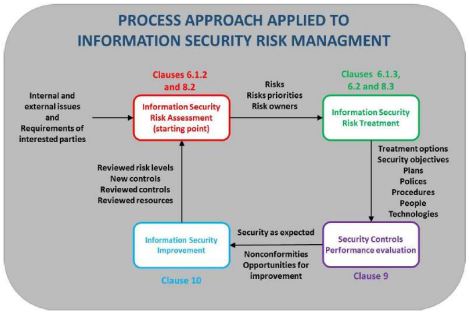
1

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 2

- In this lesson we will continue to apply elements of ISO 27001 Information Security Management System.
- Step 1 in ISO 27001 is Risk Assessment.



2
Esc

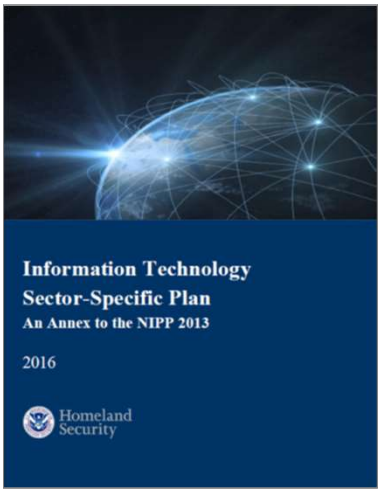
2

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 2

- **Risk exposure, in this case, refers to how many customers could be affected if an ISP is attacked.**
- The 2016 IT Sector-Specific Plan cites denial of service attack as a specific risk to ISPs.
- Let's start by looking at the Tier 2 ISPs.



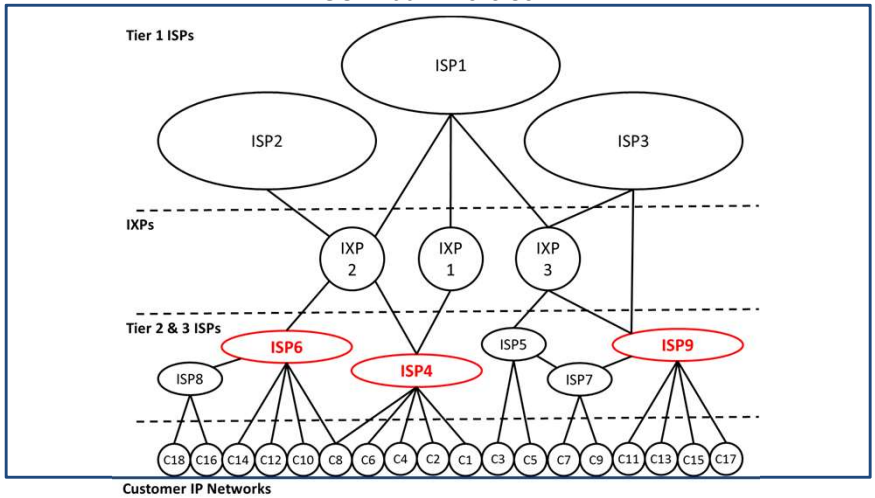
3
Esc

3

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 2



Q1: Which Tier 2 ISP has largest risk exposure based on number of customers?

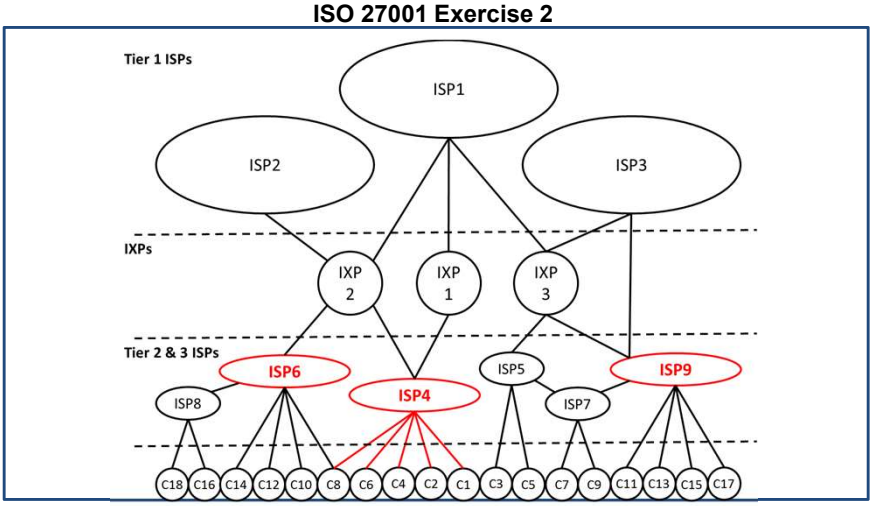
4
Esc

4

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 2



Q1: Which Tier 2 ISP has largest risk exposure based on number of customers?
A1: ISP4

5

Esc

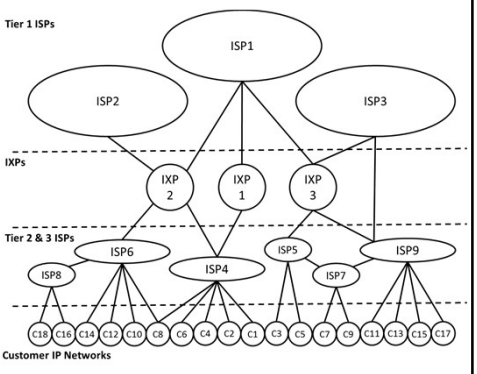
5

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 2

Generally speaking, an ISP with more external links assumes less risk.

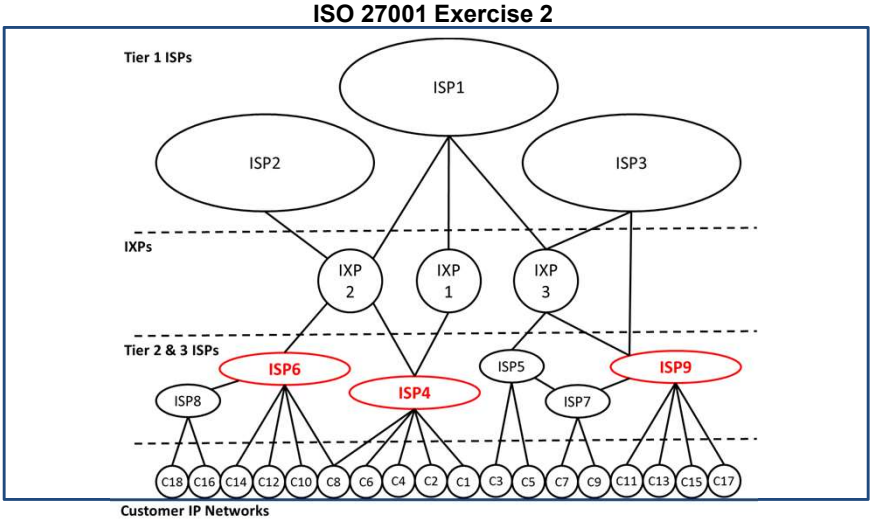


6

Esc

6

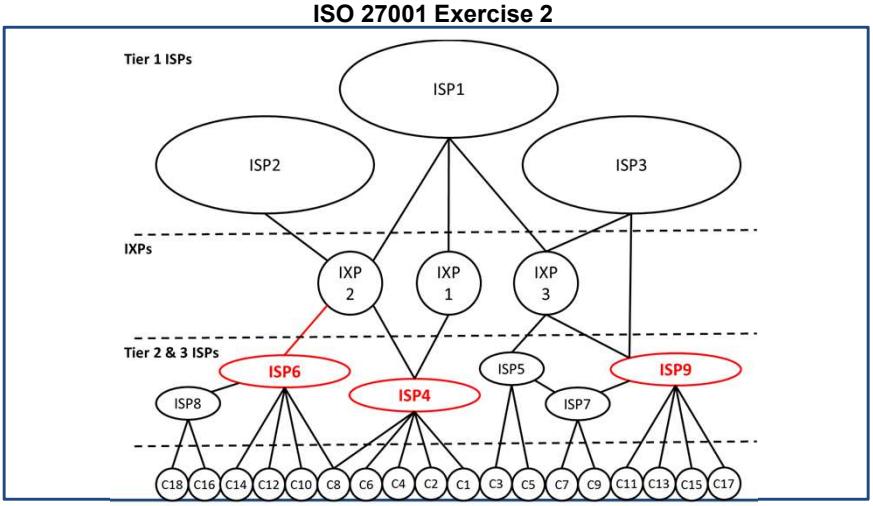
ISO 27001 Exercise 2



Q2: Which Tier 2 ISP is assuming the most risk?

7

ISO 27001 Exercise 2



Q2: Which Tier 2 ISP is assuming the most risk?

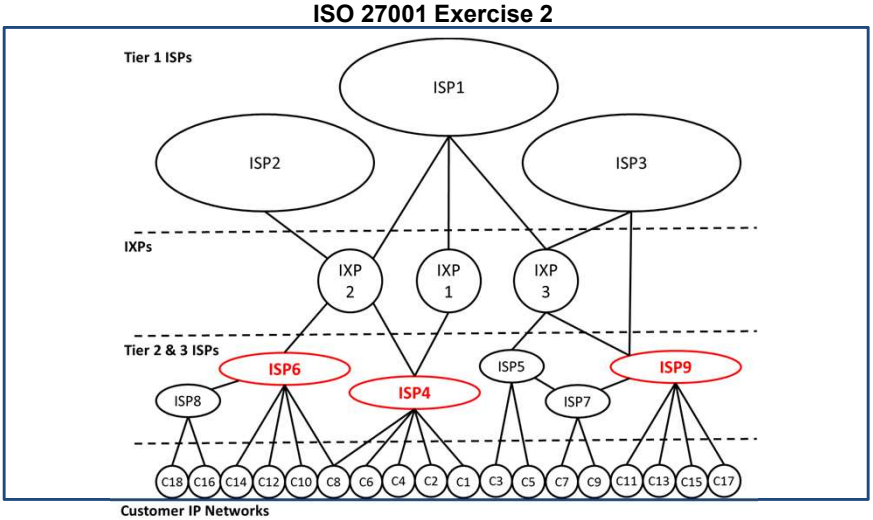
A2: ISP6

8

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 2



Q3: Which Tier 2 ISP is assuming the least amount of risk?

9

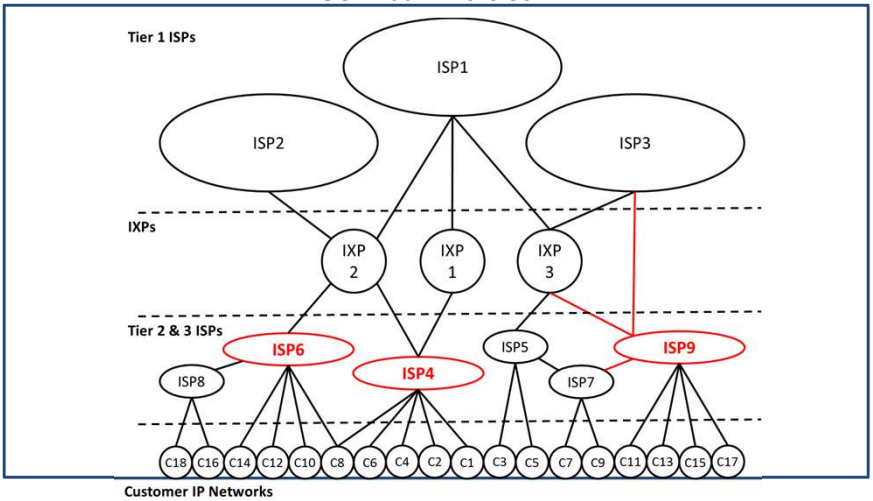
Esc

9

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 2



Q3: Which Tier 2 ISP is assuming the least amount of risk?
A3: ISP9

10

Esc

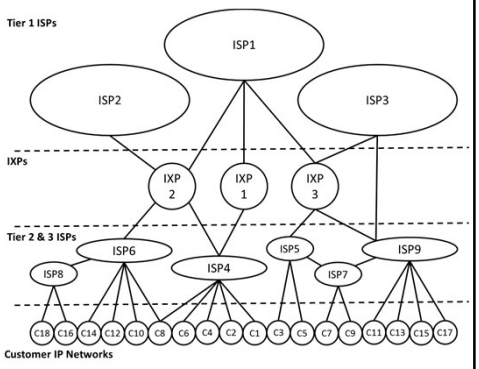
10

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 2

- **ISP9 is assuming the least amount of risk because it has the most number of external links.**
- ISP9 connects to IXP3, ISP3, and ISP7.
- In effect, ISP9 has double redundancy.
- By comparison, ISP4 has only single redundancy.
- ISP4 has only two external links.



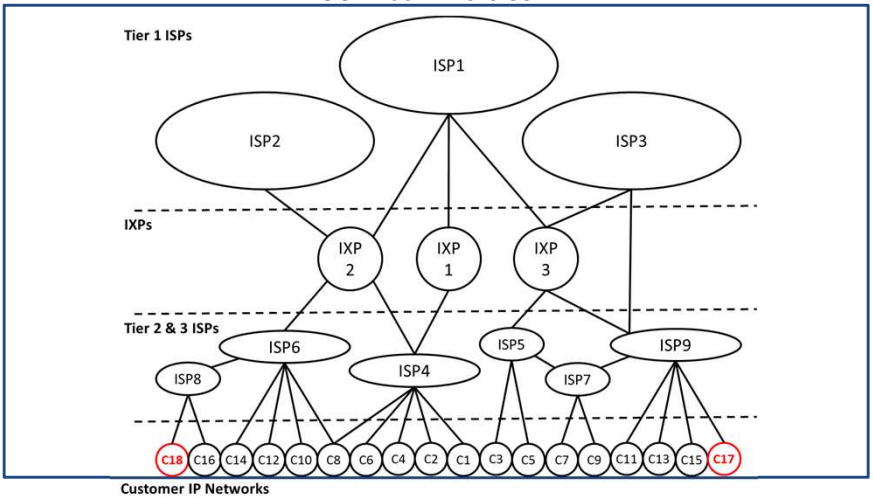
11
Esc

11

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 2

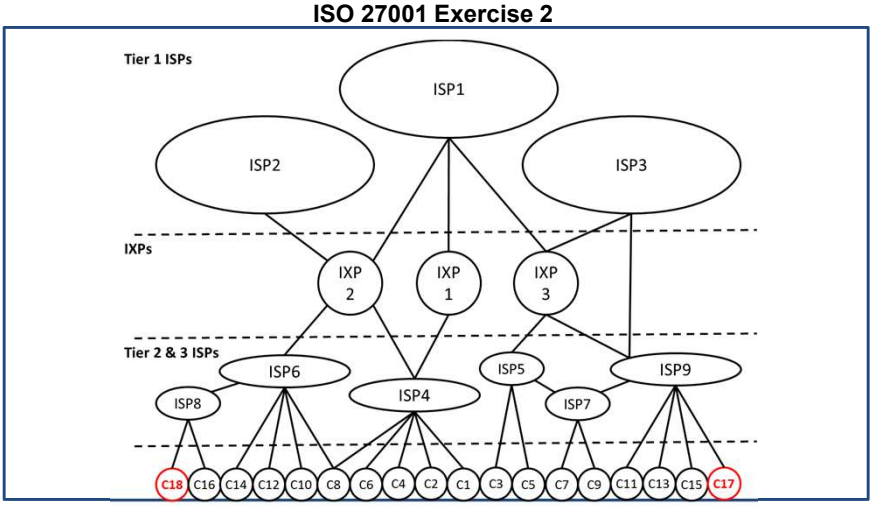


Q4: Which is more at risk of suffering an Internet outage, C18 or C17?

12
Esc

12

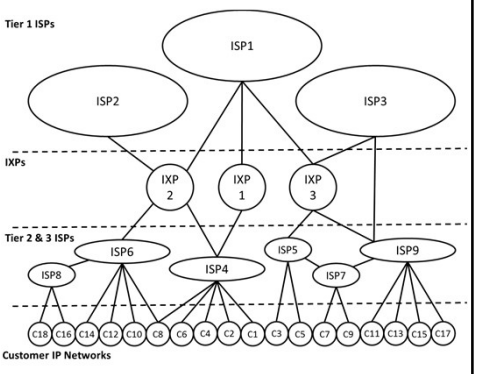
ISO 27001 Exercise 2



Q4: Which is more at risk of suffering an Internet outage, C18 or C17?
A4: C18

ISO 27001 Exercise 2

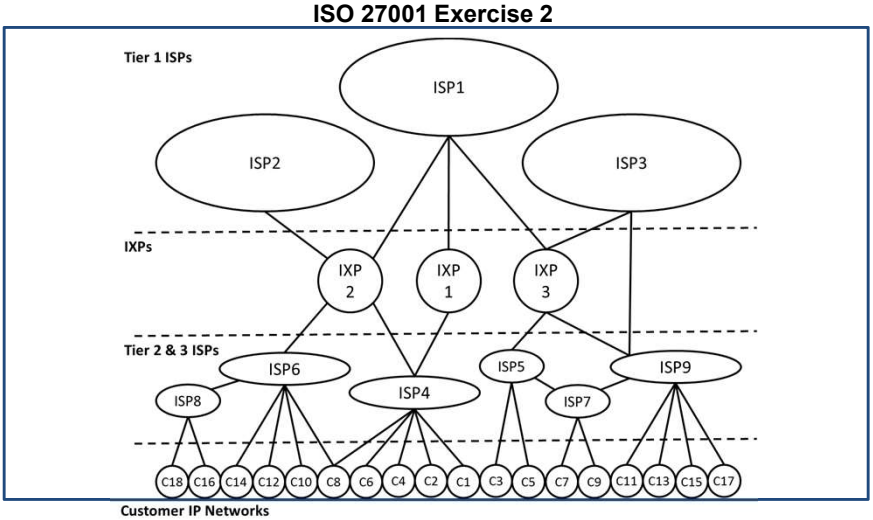
- **Customer #18 is most at risk because they connect to the Internet through ISP 6 which has no redundant links.**
- By comparison, Customer #17 is less at risk because they connect to the Internet through ISP9 which has 2 redundant links.



University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 2



Q5: Among all customers, which has least risk of suffering a disconnect?

15

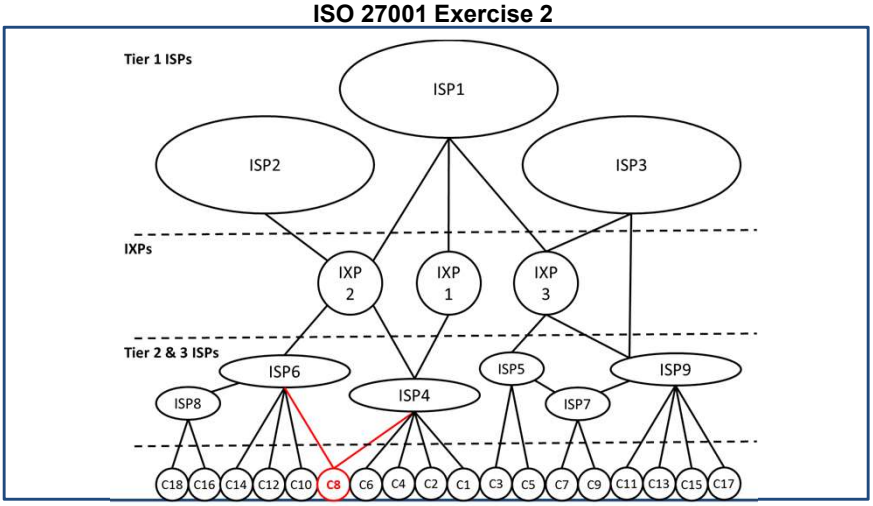
Esc

15

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 2



Q5: Among all customers, which has least risk of suffering a disconnect?
A5: C8

16

Esc

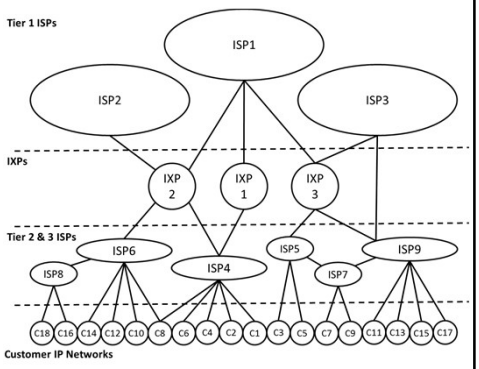
16

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 2

- Customer #8 has the least risk exposure because they are the only customer separately connected to two different ISPs.
- **Customer #8 is the only customer that doesn't have a single point of failure.**



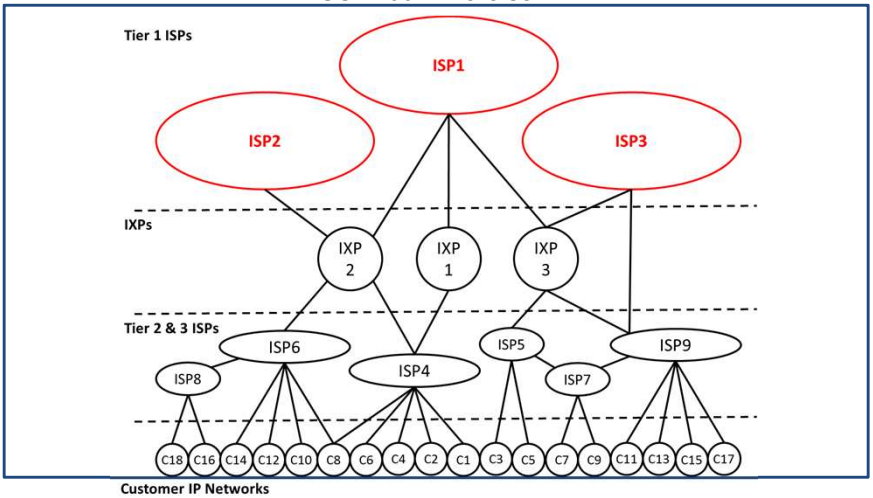
17
Esc

17

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 2



Q6: Which Tier 1 ISP is least critical?

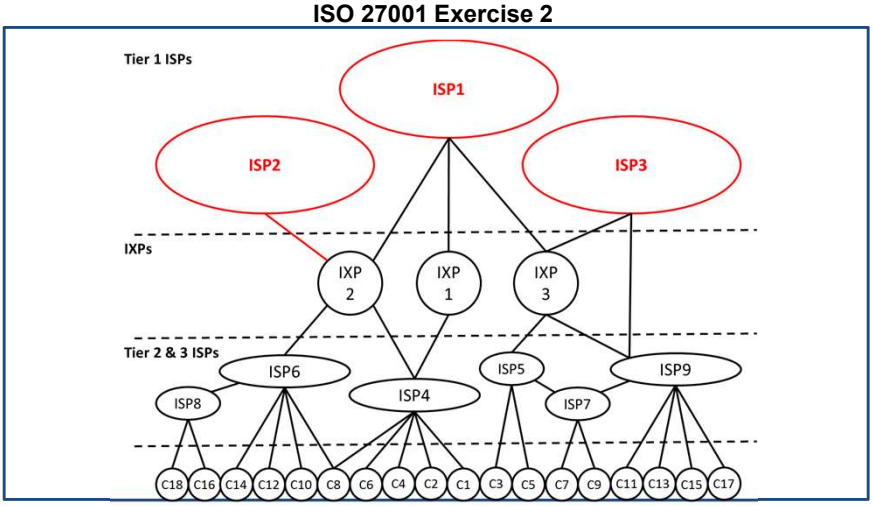
18
Esc

18

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 2



Q6: Which Tier 1 ISP is least critical?
A6: ISP2

19

Esc

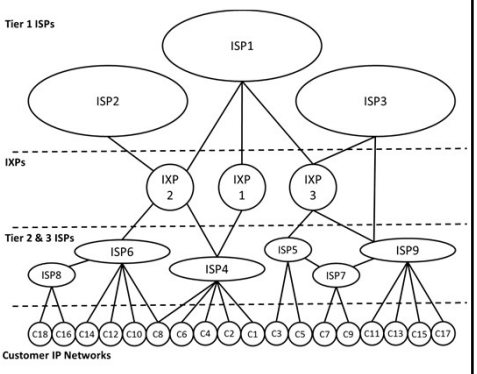
19

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 2

- **ISP2 is least critical because it can be removed from the network without impairing traffic to other parts of the network.**
- Realistically, it is highly unlikely that any Tier 1 ISP would be so isolated as ISP2.
- Of course the Internet architecture depicted in our diagram is just for illustration purposes.
- Any resemblance to reality is purely coincidental.



20

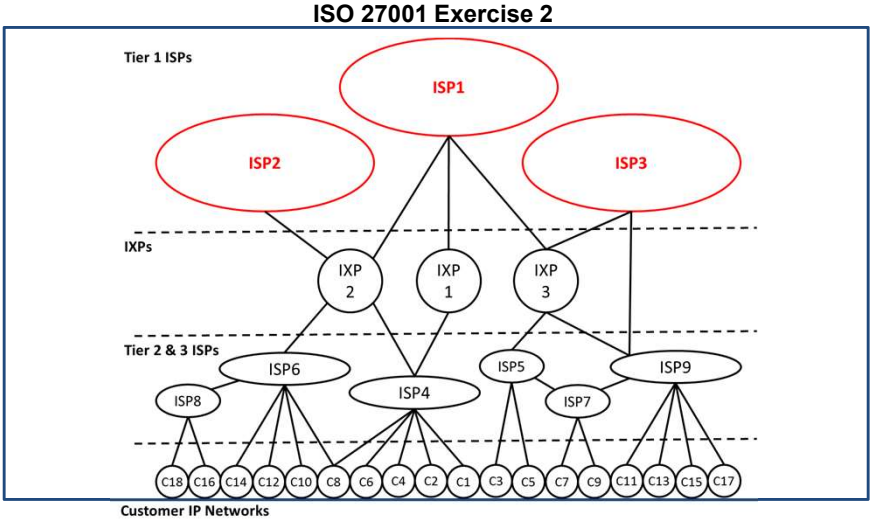
Esc

20

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 2



Q7: Which Tier 1 ISP is most critical?

21

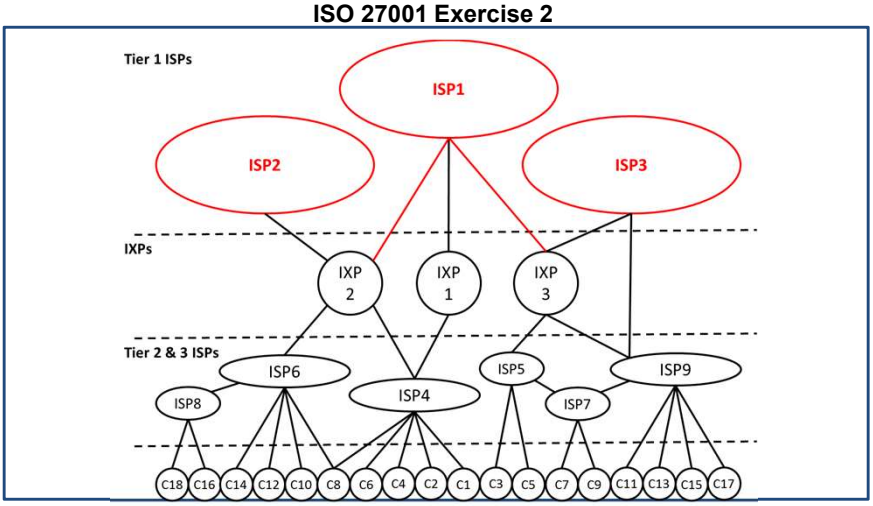
Esc

21

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 2



Q7: Which Tier 1 ISP is most critical?
A7: ISP1

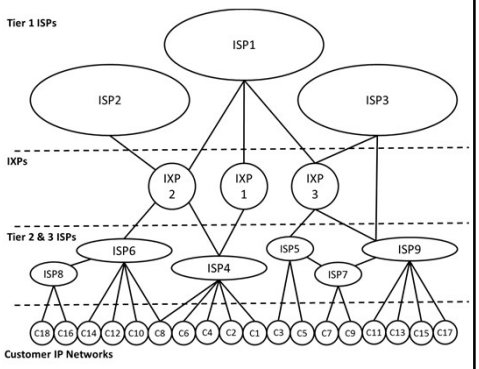
22

Esc

22

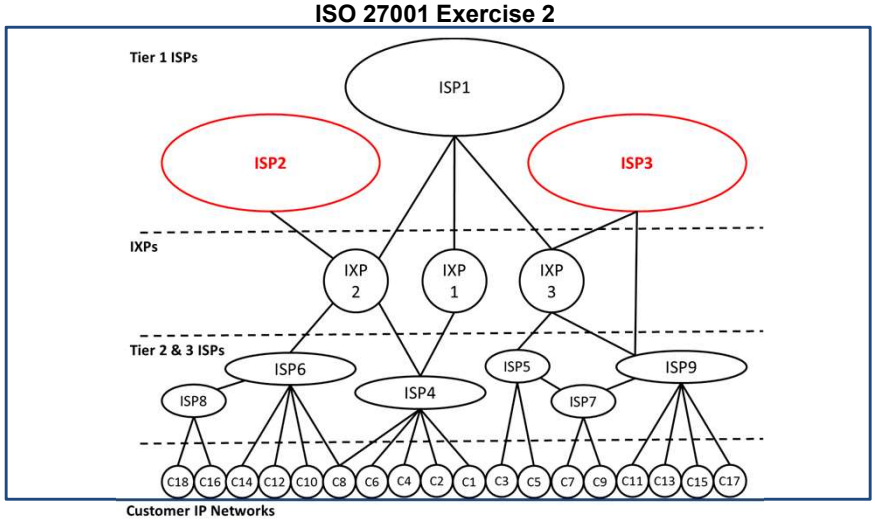
ISO 27001 Exercise 2

ISP 1 is most critical because it not only has the most external links, but it is also the only bridge linking the "even" side of the network with the "odd" side of the network.



23

ISO 27001 Exercise 2



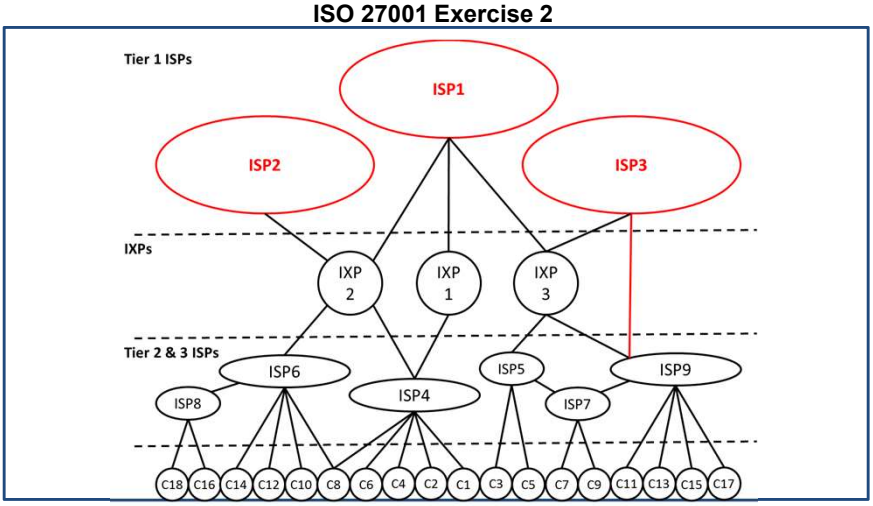
Q8: Which is more critical, ISP3 or ISP2?

24

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 2



Q8: Which Tier 1 ISP is most critical?
A8: ISP3

25

Esc

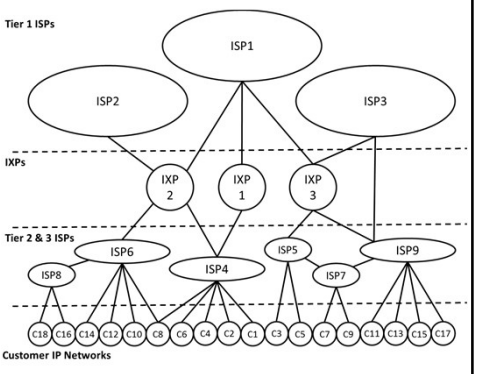
25

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 2

- **ISP3 is more critical than ISP2 because it offers a redundant path to ISP9.**
- ISP2 offers no redundancy anywhere.



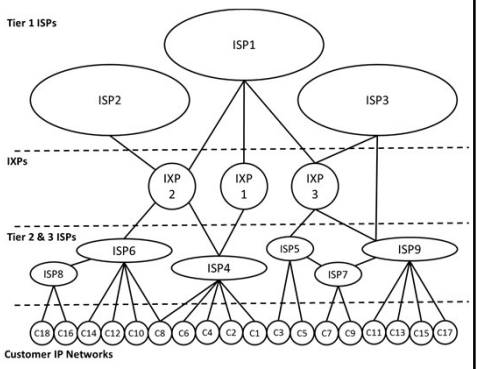
26

Esc

26

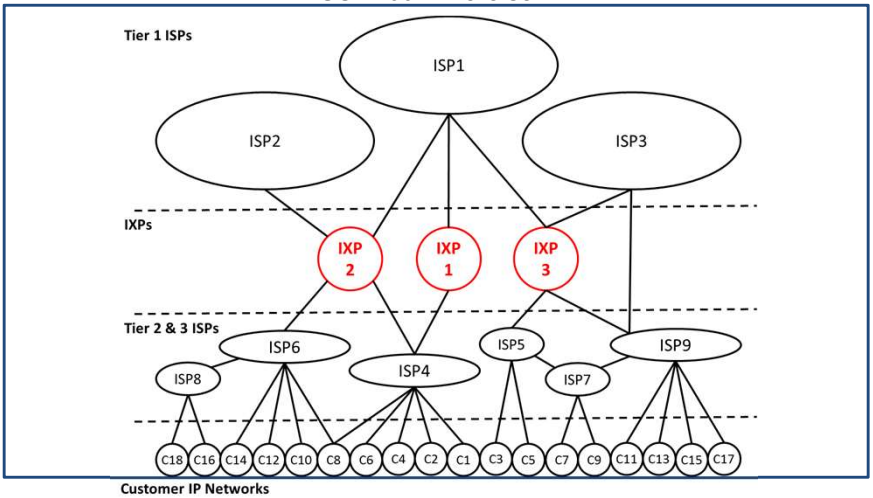
ISO 27001 Exercise 2

Okay, let's take another look at criticality with respect to the IXPs.



27

ISO 27001 Exercise 2



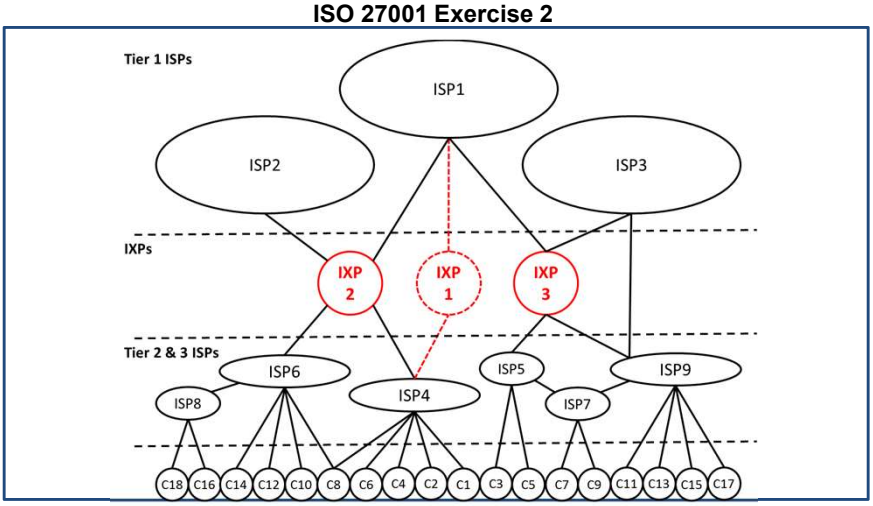
Q9: Which IXP is least critical?

28

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 2



Q9: Which IXP is least critical?
A9: IXP1

29

Esc

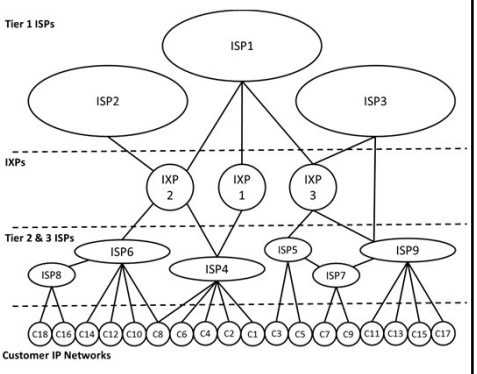
29

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

ISO 27001 Exercise 2

IXP1 is least critical because it could be removed without affecting network traffic.

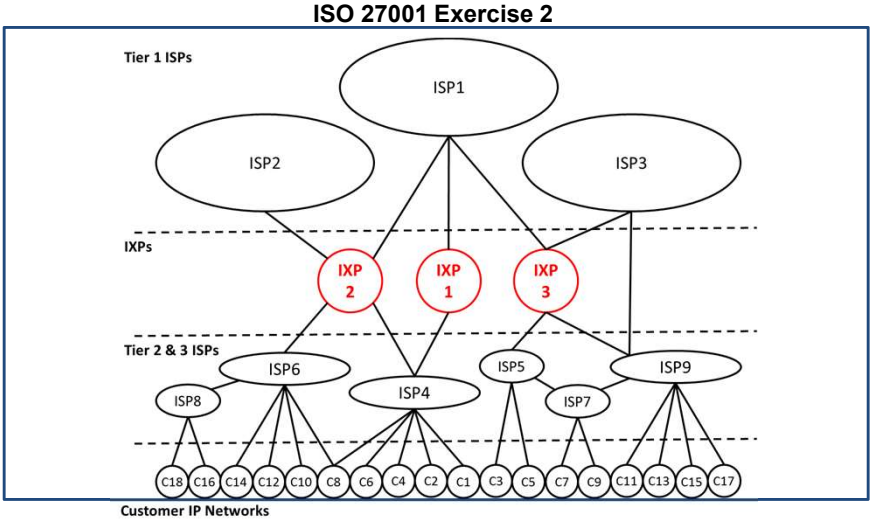


30

Esc

30

ISO 27001 Exercise 2



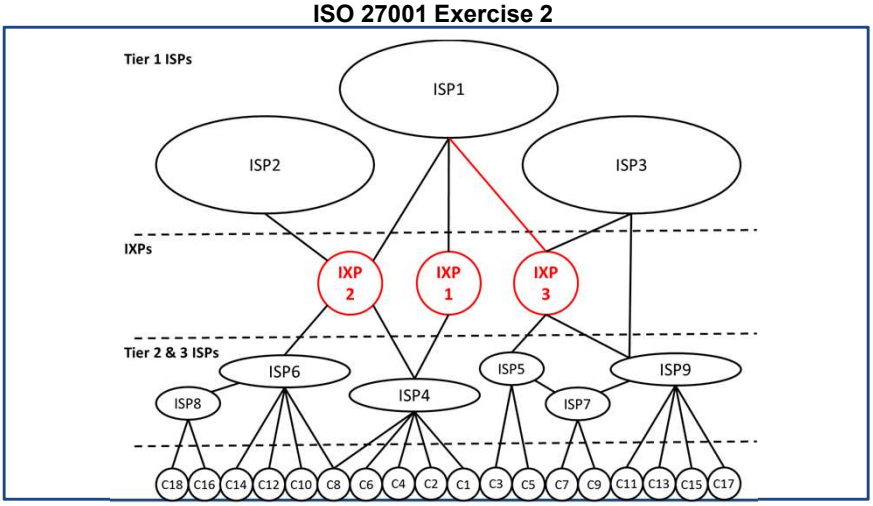
Q10: Which IXP is most critical?

31

Esc

31

ISO 27001 Exercise 2



Q10: Which IXP is most critical?

A10: IXP3

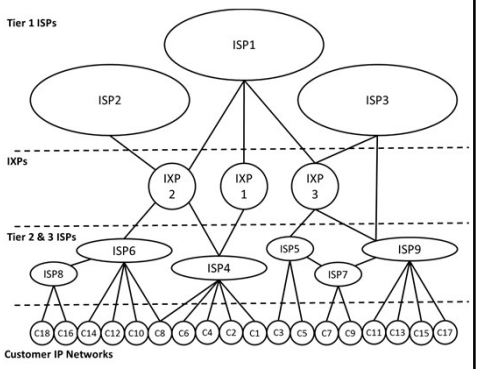
32

Esc

32

ISO 27001 Exercise 2

IXP3 is most critical because it provides the only bridge linking the "even" side of the network with the "odd" side.



Conclusion

Questions?