Wireless Systems Security

EE/NiS/TM-584-A/WS

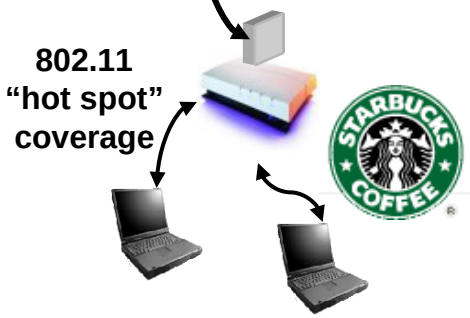
Bruce McNair
bmcnair@stevens.edu

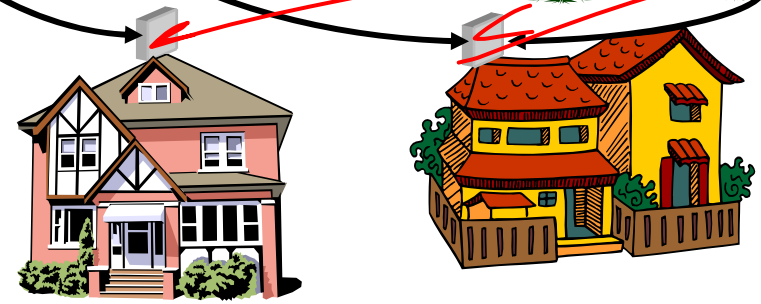
Week 11

Case Study 7

Case 7 – Wireless Metropolitan Area Networks (W-MANs) 802.16

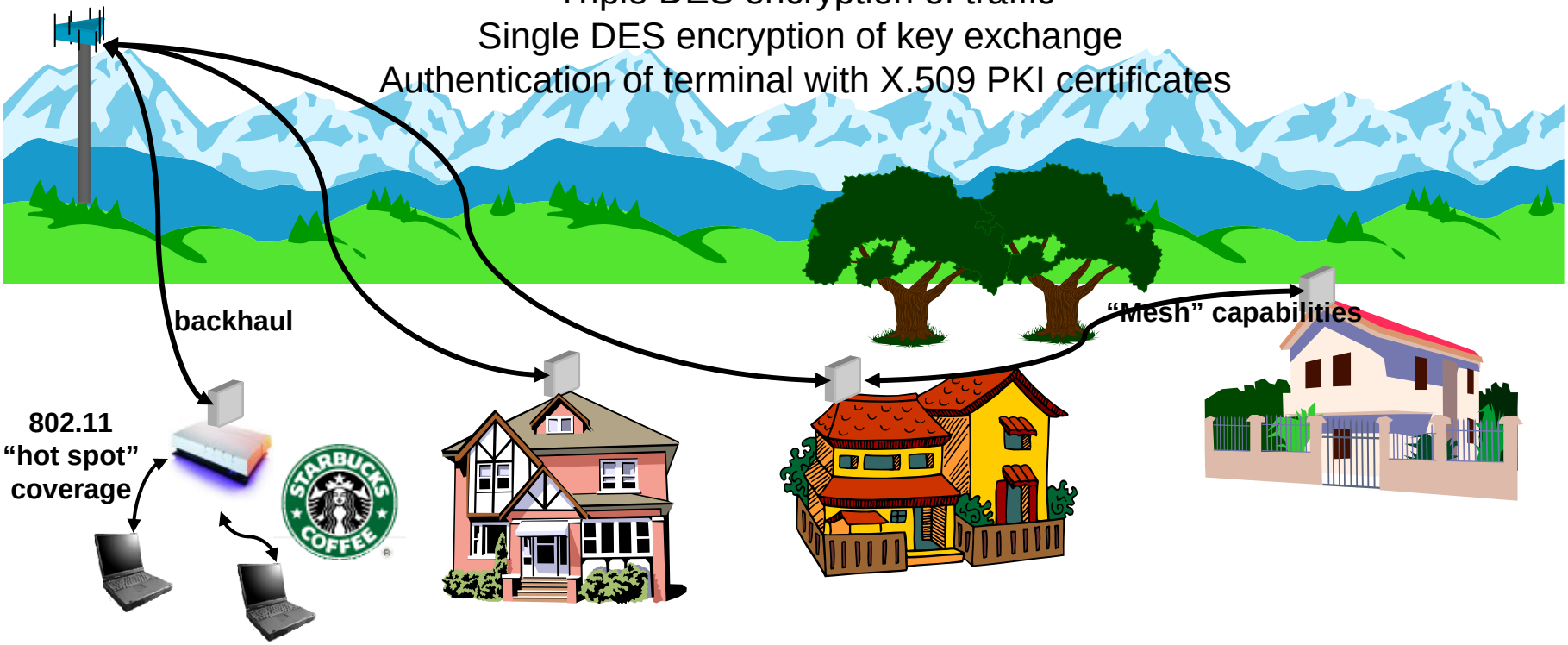
802.16a: 2-11 GHz 256/2048 carrier OFDM,
802.16.1: 10 – 66 GHz LOS
120 Mb/s capacity
T1+ user data, multiple voice channels, Wireless Local Loop
Triple DES encryption of traffic
Single DES encryption of key exchange
Authentication of terminal with X.509 PKI certificates



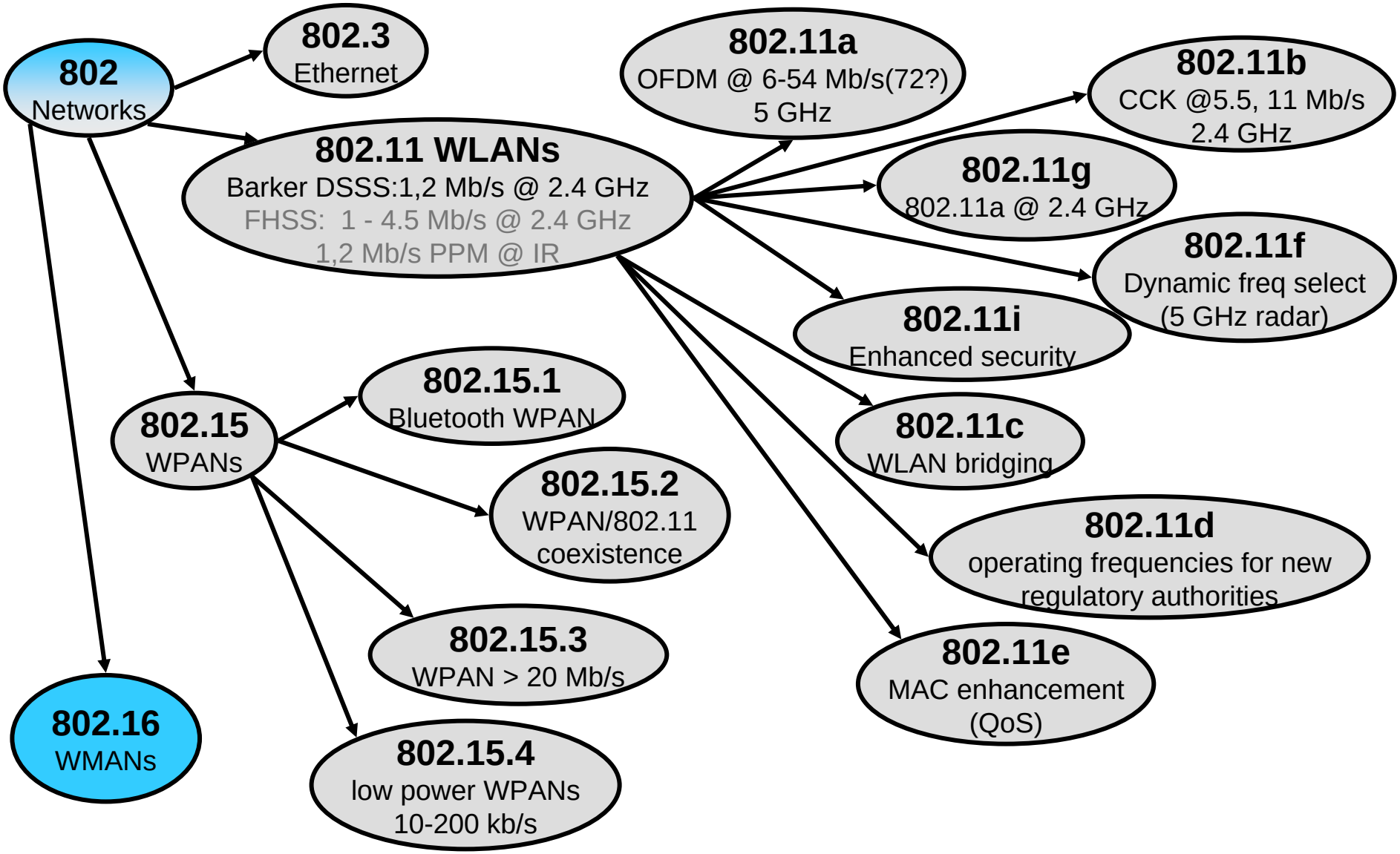


Case 7 –
Wireless Metropolitan Area Networks (W-MANs)
802.16

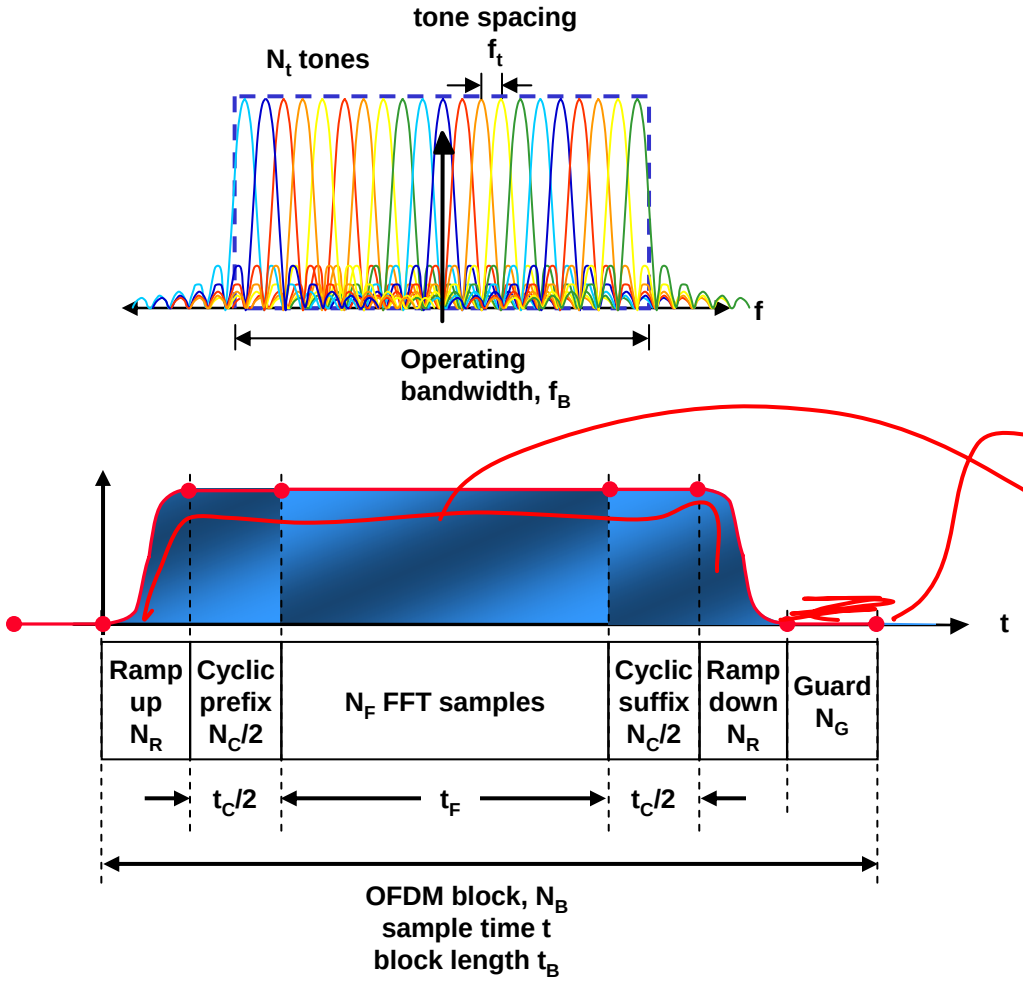
802.16a: 2-11 GHz 256/2048 carrier OFDM,
802.16.1: 10 – 66 GHz LOS
120 Mb/s capacity
T1+ user data, multiple voice channels, Wireless Local Loop
Triple DES encryption of traffic
Single DES encryption of key exchange
Authentication of terminal with X.509 PKI certificates



IEEE 802 Standards (Alphabet Soup)



OFDM Basics



Total bandwidth $f_B = N_t f_t$

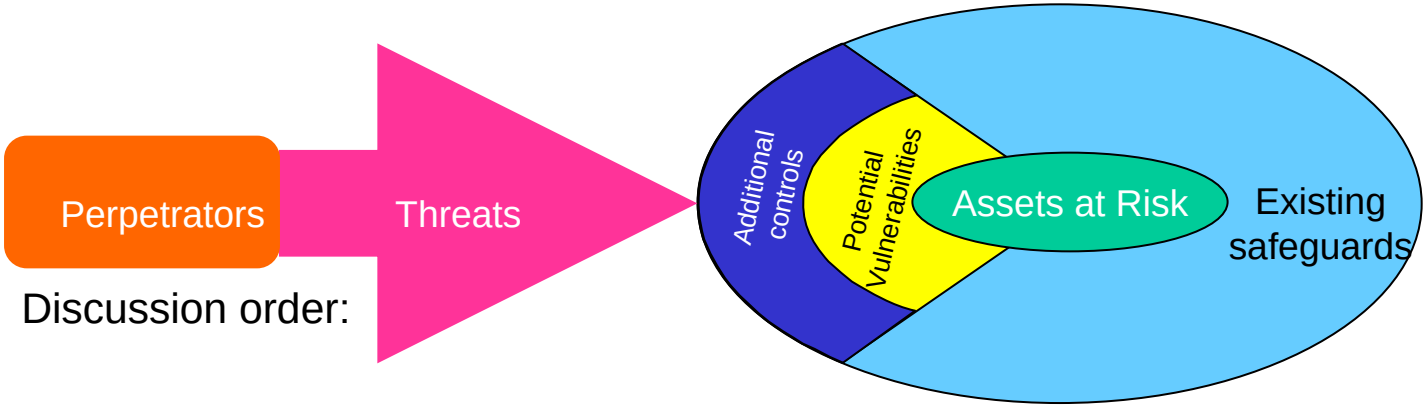
Tone spacing vs active block time $f_t = \frac{1}{t_F}$

$N_B = 2N_R + N_C + N_G + N_F$

Block efficiency $\eta = \frac{N_F}{N_B} = \frac{N_F}{N_F + N_C + 2N_R + N_G}$

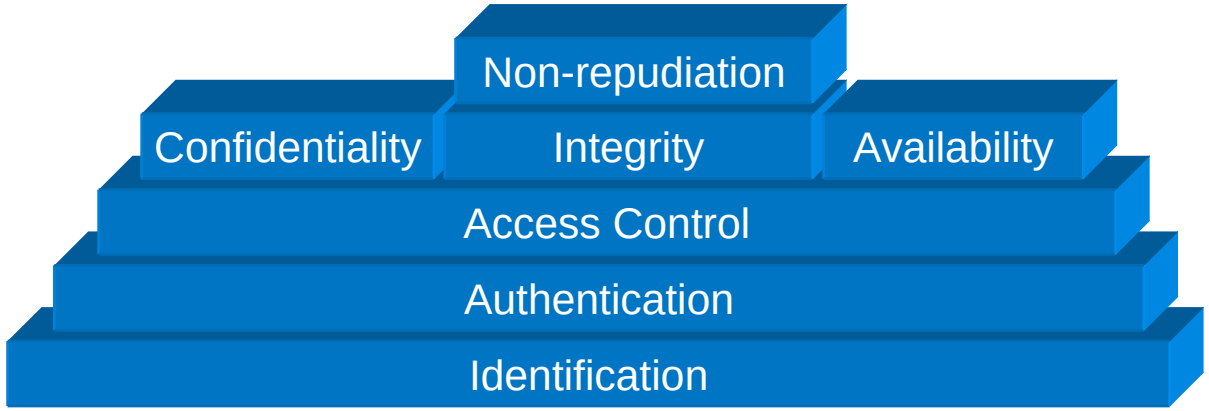
Tolerance to delay spread $\approx t_C \propto N_C$

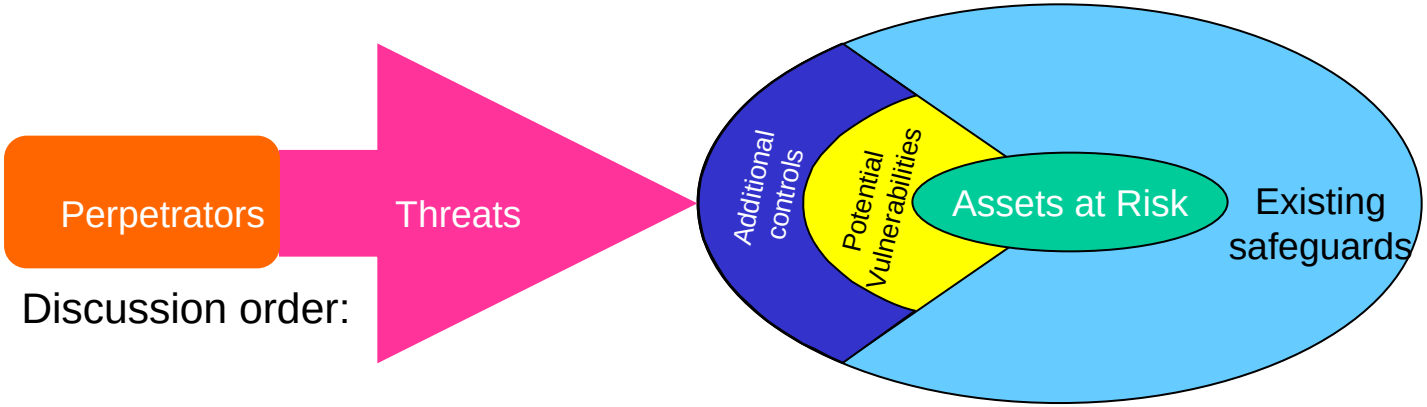
Raw capacity for M-ary tone modulation $N_t M$



Discussion order:

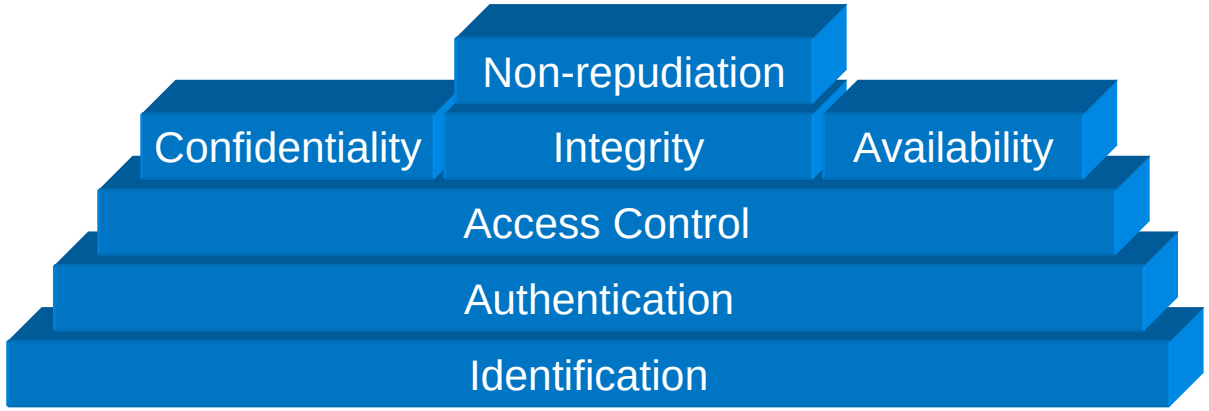
- Assets
- Perpetrators
- Threats
- Existing Safeguards
- Potential Vulnerabilities
- Additional Security Controls

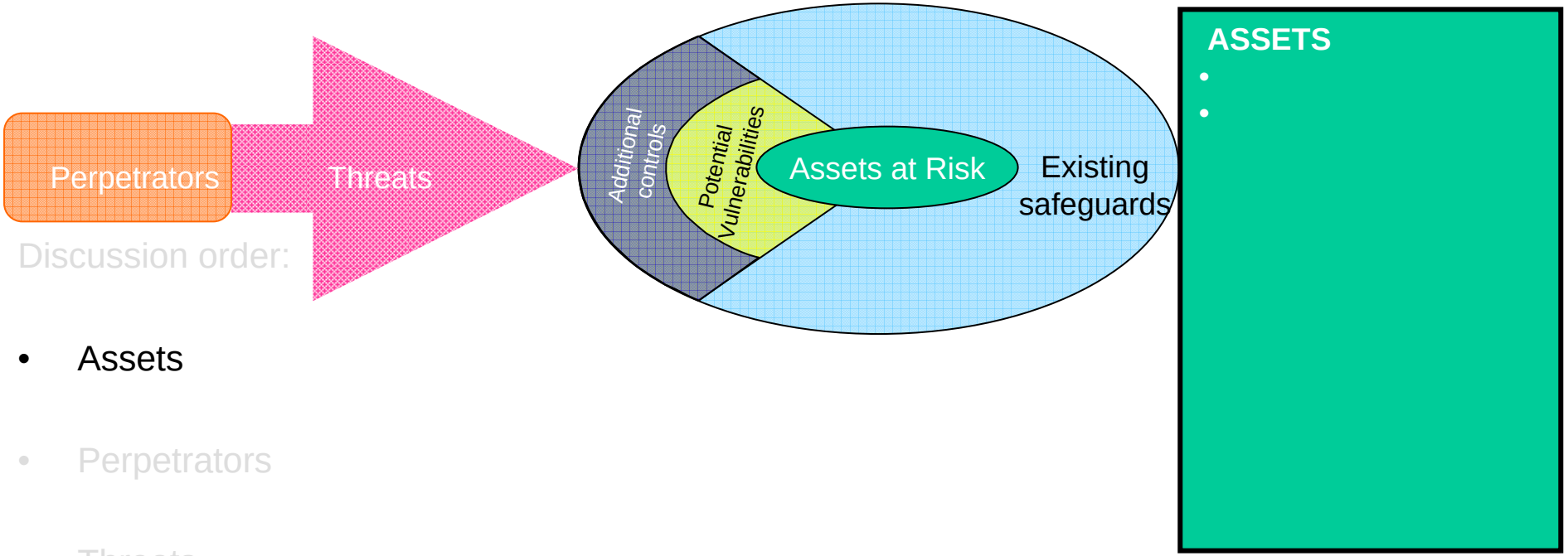




Discussion order:

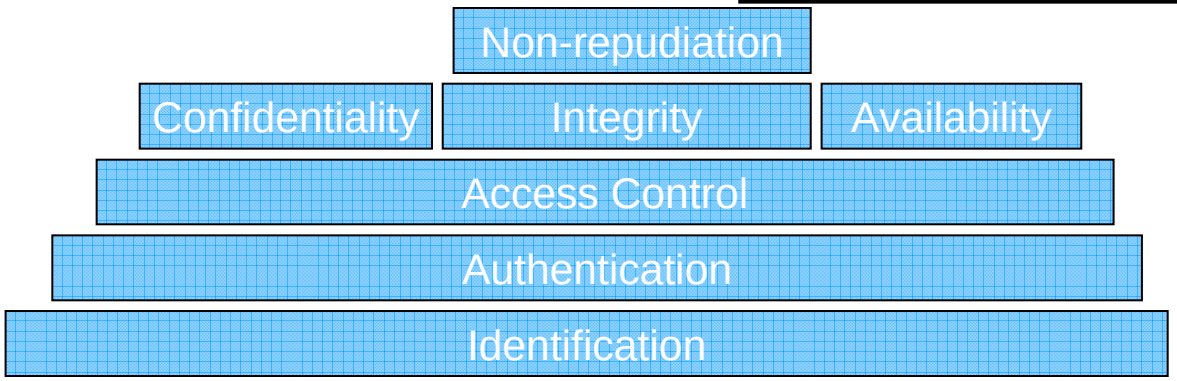
- Assets
- Perpetrators
- Threats
- Existing Safeguards
- Potential Vulnerabilities
- Additional Security Controls

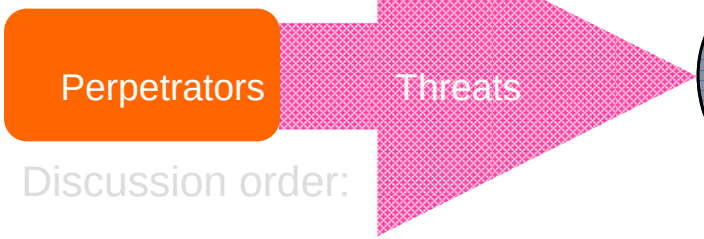


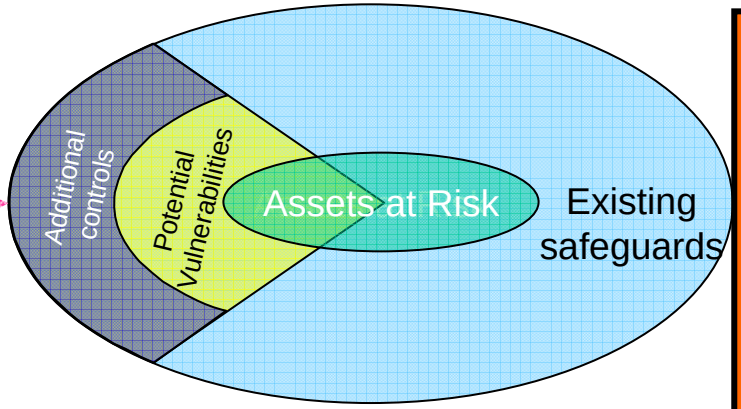


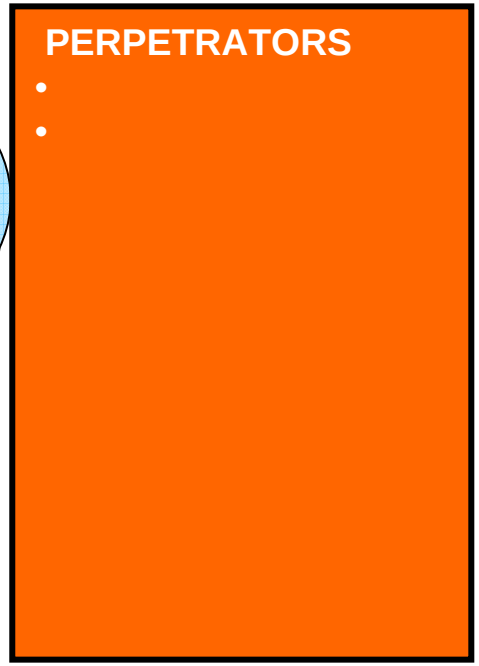
Discussion order:

- Assets
- Perpetrators
- Threats
- Existing Safeguards
- Potential Vulnerabilities
- Additional Security Controls



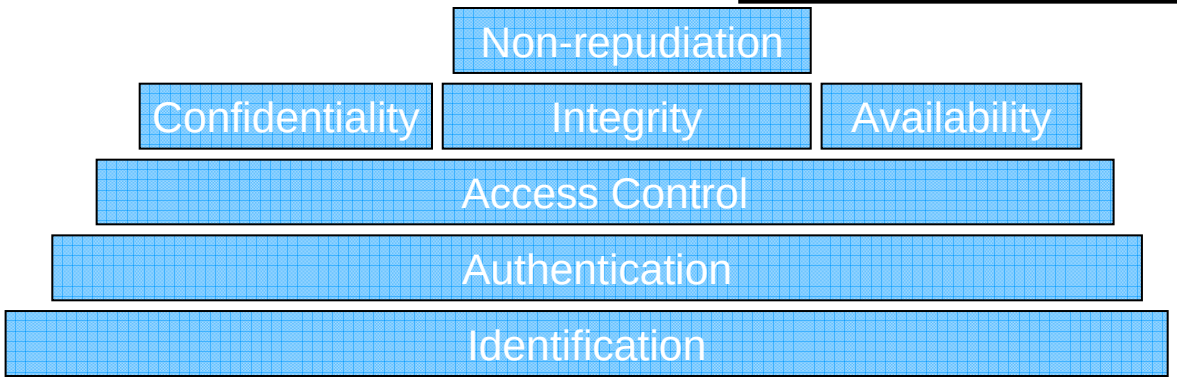


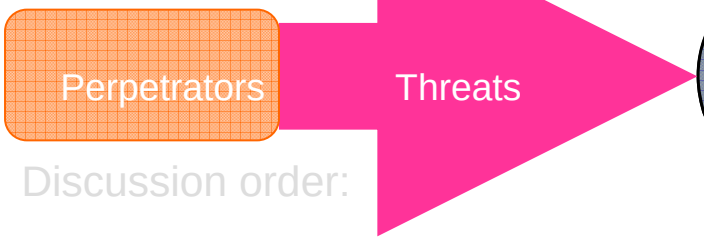


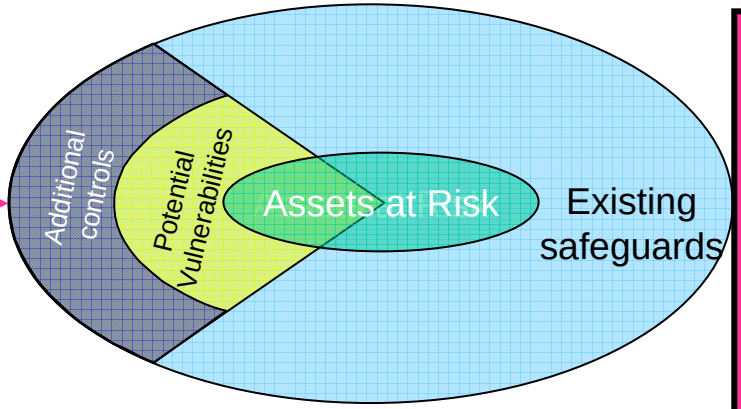


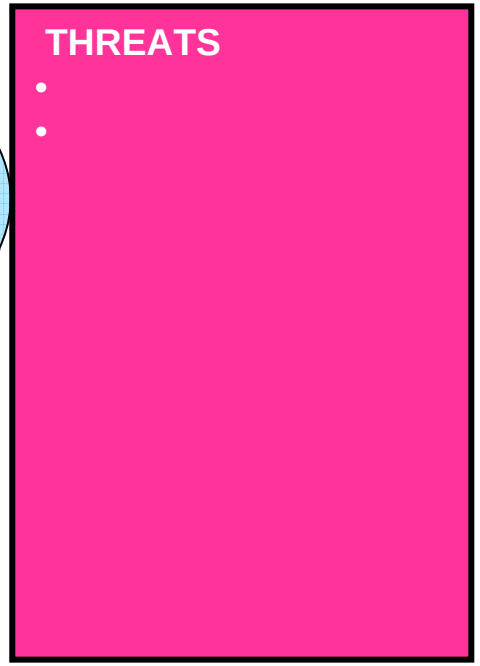
Discussion order:

- Assets
- Perpetrators
- Threats
- Existing Safeguards
- Potential Vulnerabilities
- Additional Security Controls



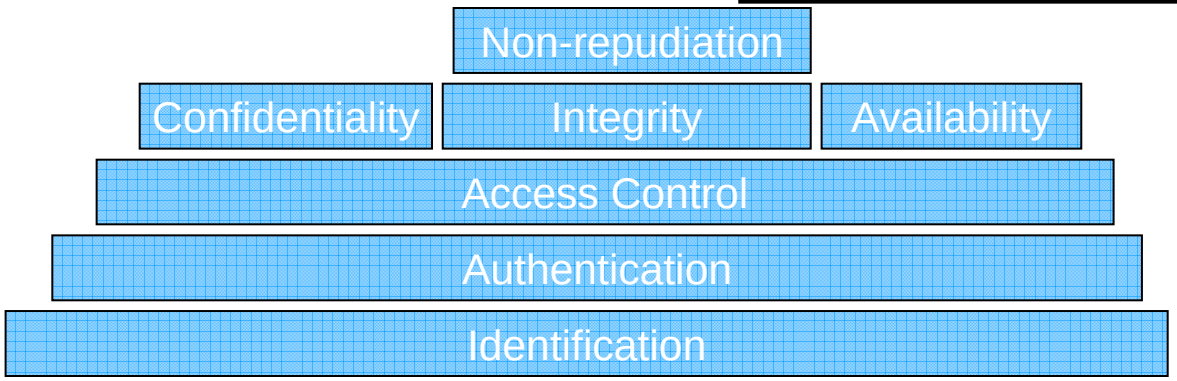


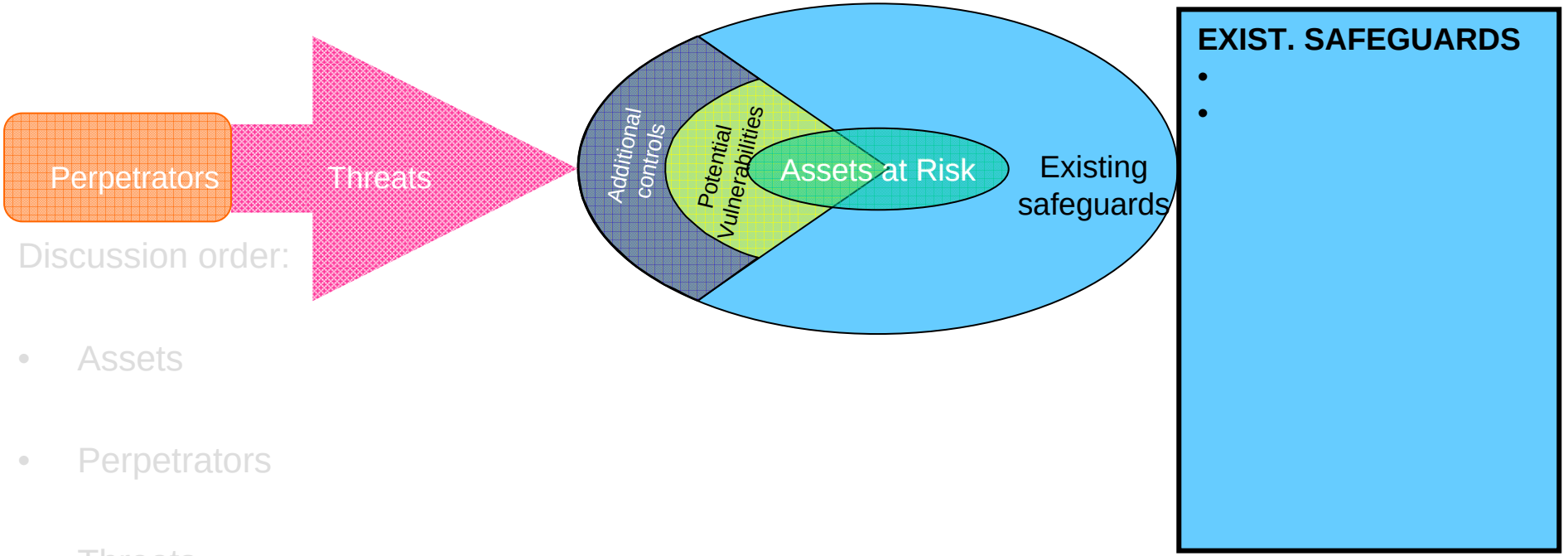




Discussion order:

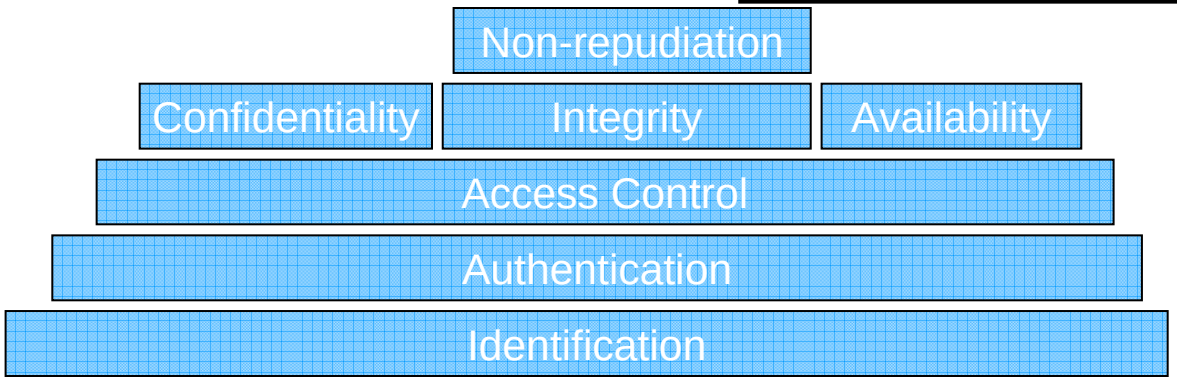
- Assets
- Perpetrators
- Threats
- Existing Safeguards
- Potential Vulnerabilities
- Additional Security Controls

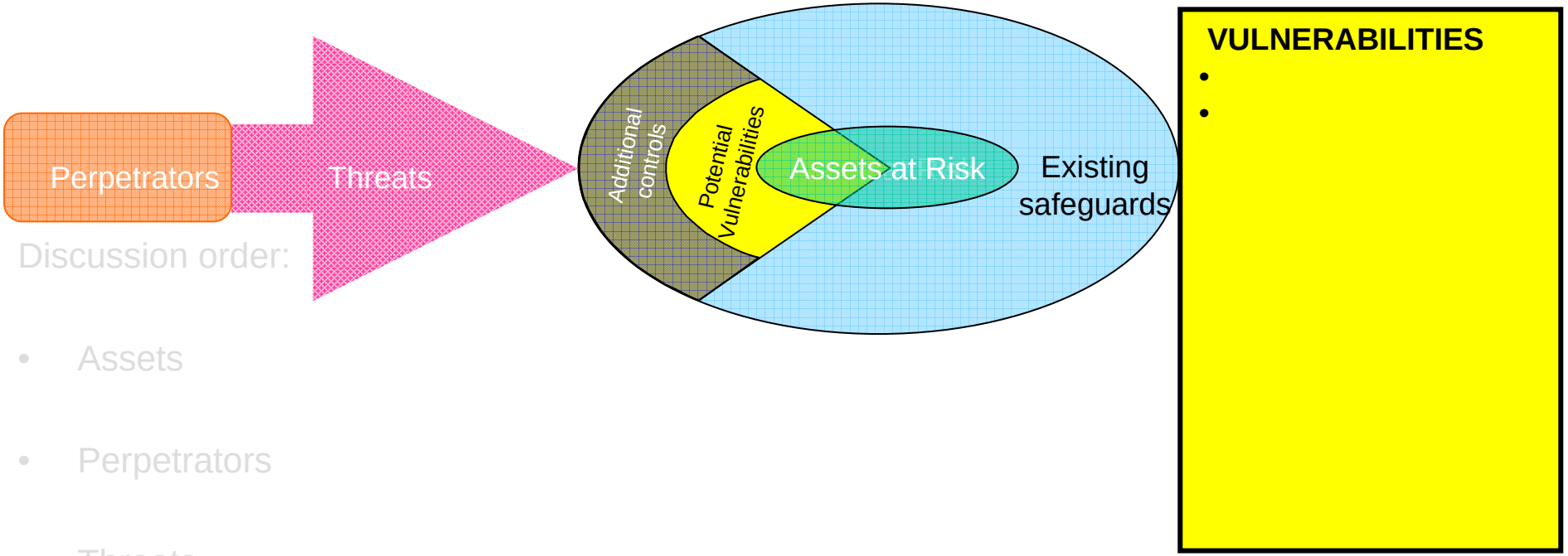




Discussion order:

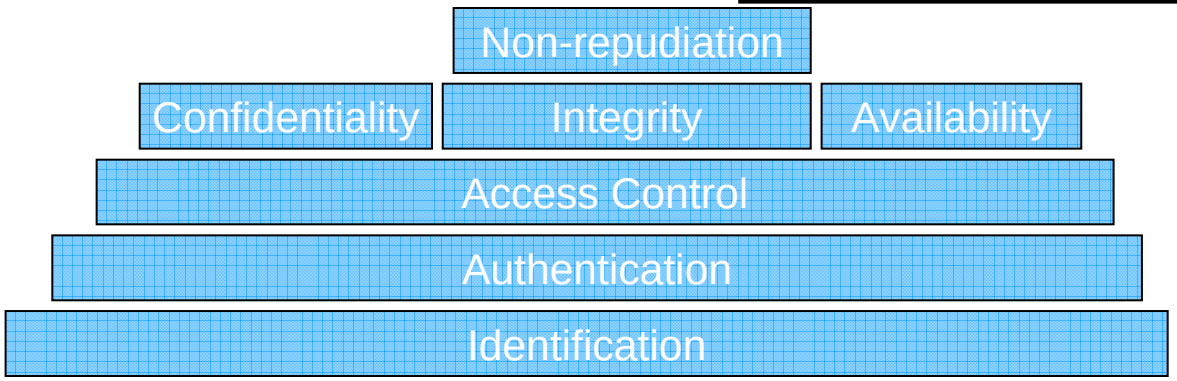
- Assets
- Perpetrators
- Threats
- Existing Safeguards
- Potential Vulnerabilities
- Additional Security Controls

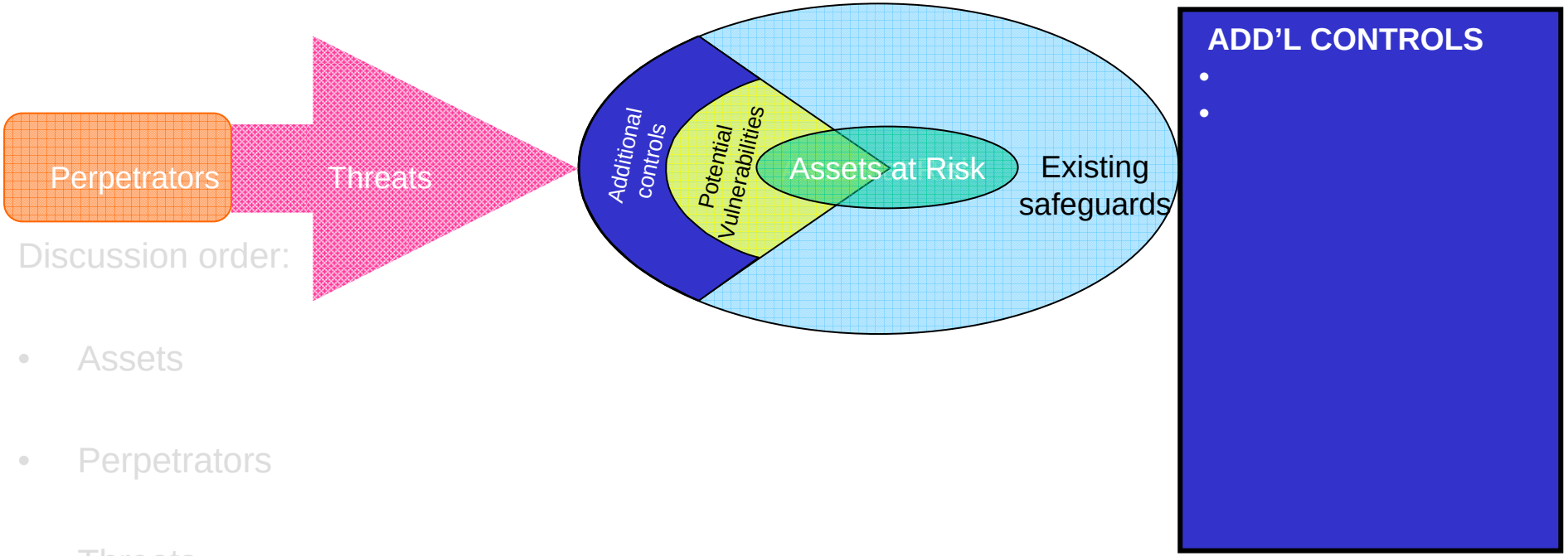




Discussion order:

- Assets
- Perpetrators
- Threats
- Existing Safeguards
- Potential Vulnerabilities
- Additional Security Controls





Discussion order:

- Assets
- Perpetrators
- Threats
- Existing Safeguards
- Potential Vulnerabilities
- Additional Security Controls