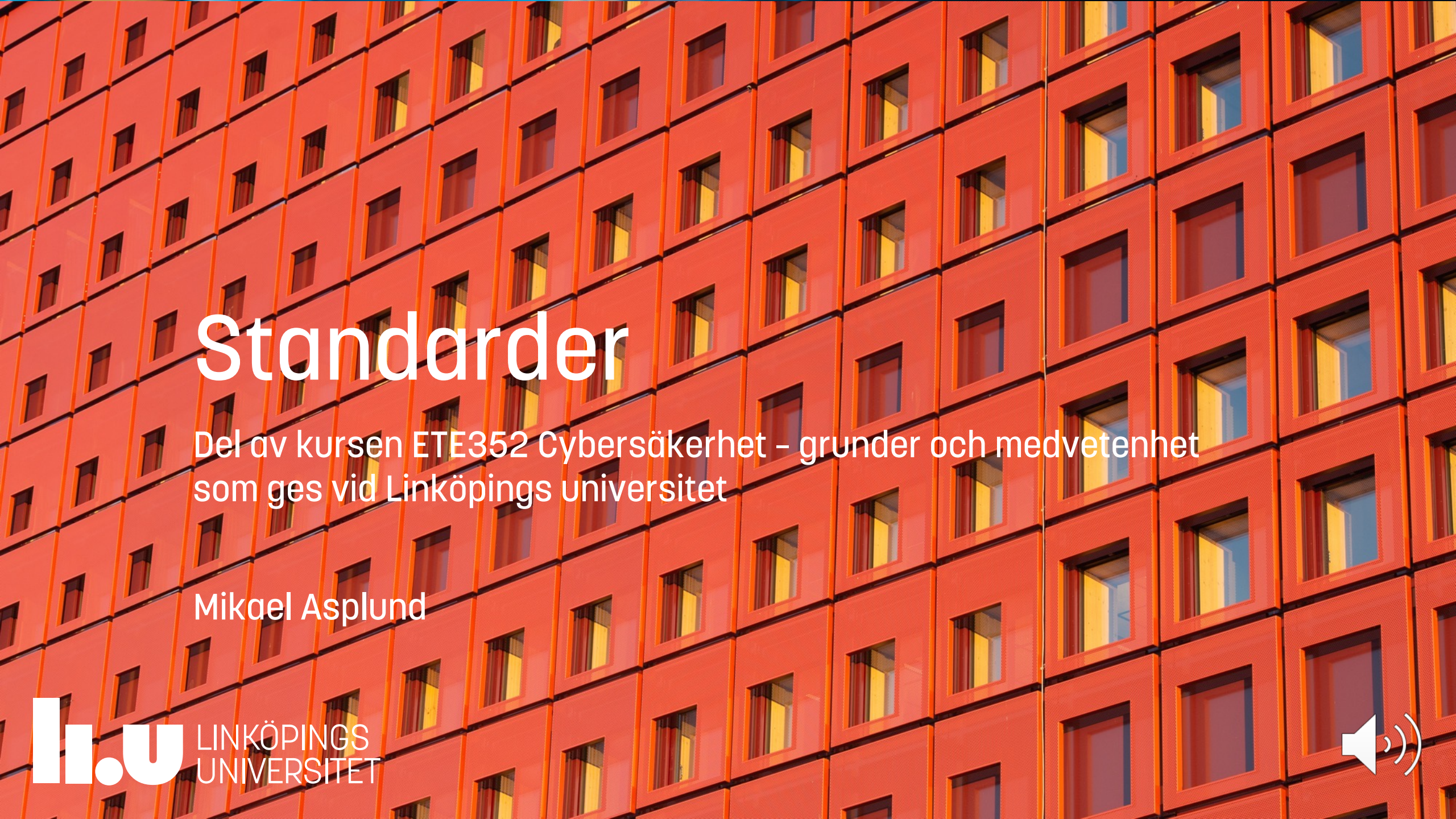

Standarder

Del av kursen ETE352 Cybersäkerhet – grunder och medvetenhet som ges vid Linköpings universitet

Mikael Asplund

LINKÖPINGS UNIVERSITET

Varför standarder?

- Gemensamt språk
- Best practice
- Hjälper att inte missa detaljer

Viktiga standarder

- Common Criteria (CC)
- ISO 270XX familjen
- NIST CSF
- Industrispecifika
  - IEC 62443
  - ISO/SAE 21434
  - PCI DSS

Common Criteria (ISO 15408)

- Harmonisering mellan Europa, USA och Kanada
- Fokus på **produkt**
- Säkerhetsegenskaper definieras genom en **skyddsprofil**
- Möjliggör oberoende **certifiering** med avseende på uppställda krav

ISO 27001

- Egentligen en hel familj av standarder – 27001-27021
  - Dessutom: 2703x, 2704x, 2705x
- Fokus på ledningssystem för säkerhet
- Normativa krav på ISMS för att minska organisationens risk

Begränsningar

- Omfattande - dyrt att genomföra
- Ofta inte tillräckligt
- Öppet för tolkning
- Skillnad mellan standard och verklighet

https://cybersakerhet-grund.ida.liu.se

LINKÖPINGS UNIVERSITET