System Security Group | Lancaster University

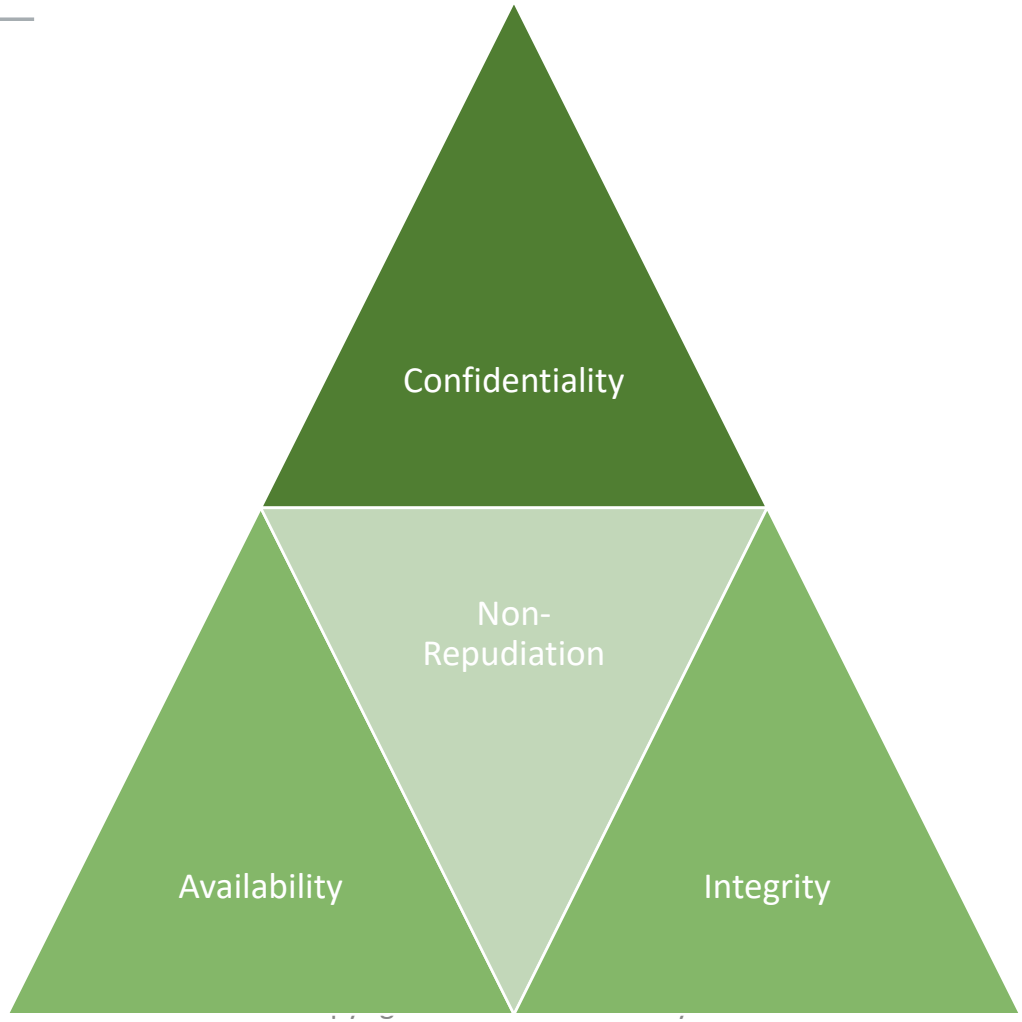
# Introduction to Cybersecurity Risk Management

# Aims

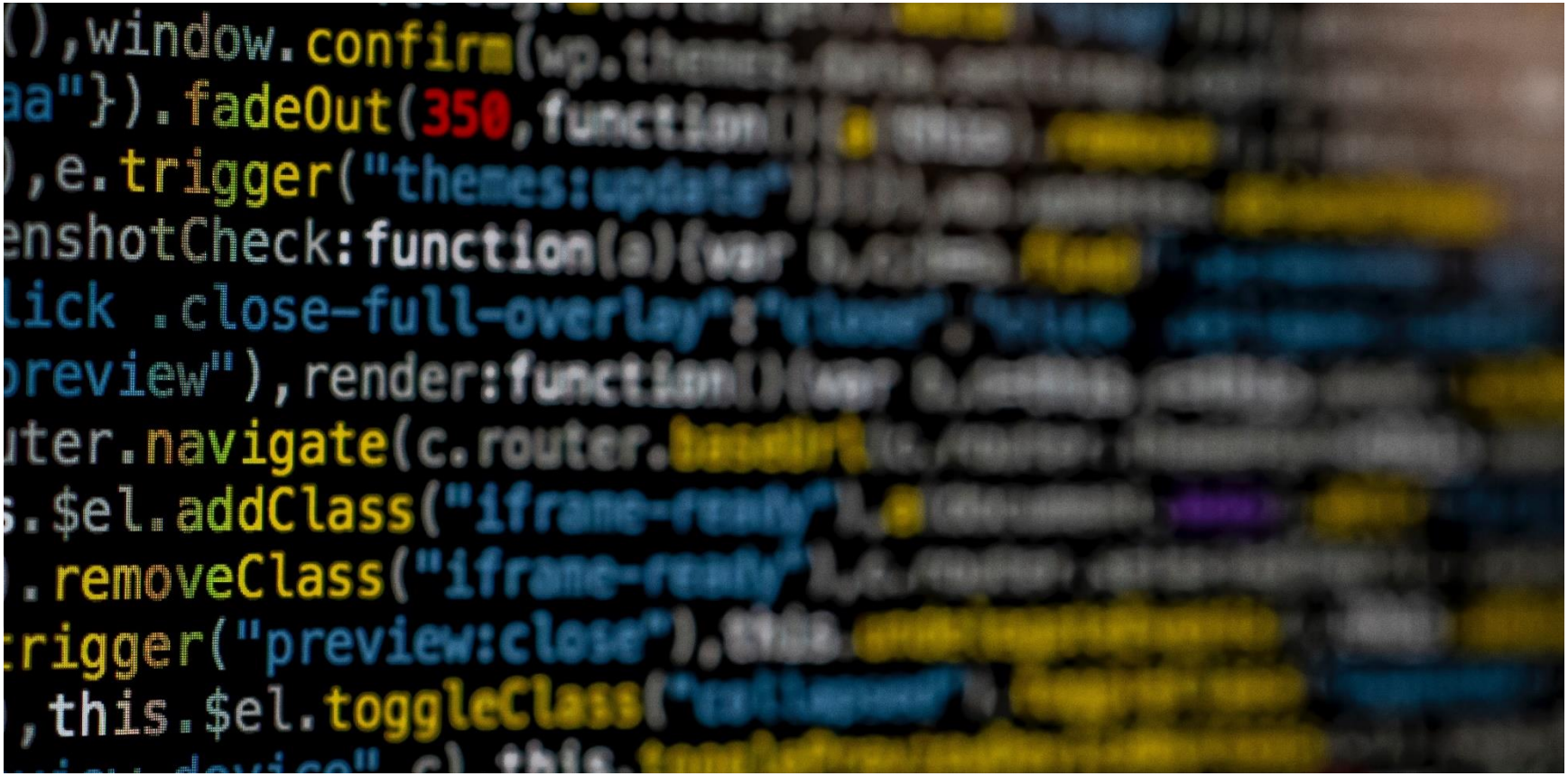
- Understand the fundamental topics and key terms
- Understand the importance of risk management in defence and protection of systems

# Confidentiality, Integrity and Availability with Non-Repudiation





# What is a Cyber Attack?



# Threat Agents, Threats and Attacks

System Security Group | Lancaster University


- Threat Agents gives rise to a Threats
  - Threats are the possibility of damaging actions
    - Threats are made against socio-technical systems

# Vulnerabilities, Exploits, Payloads and Actions






- Vulnerabilities are used by Exploits
  - Exploits carry a Payload
    - Payloads achieves the intended objective

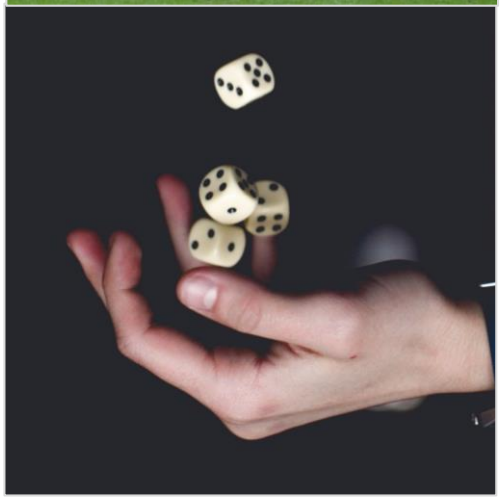
# What is Risk?

# Sources of Uncertainty

Who is the Attacker?

What is there Goal?

How likely is it they will succeed?



What is the impact if they do?

# Risk Management and Risk Assessment

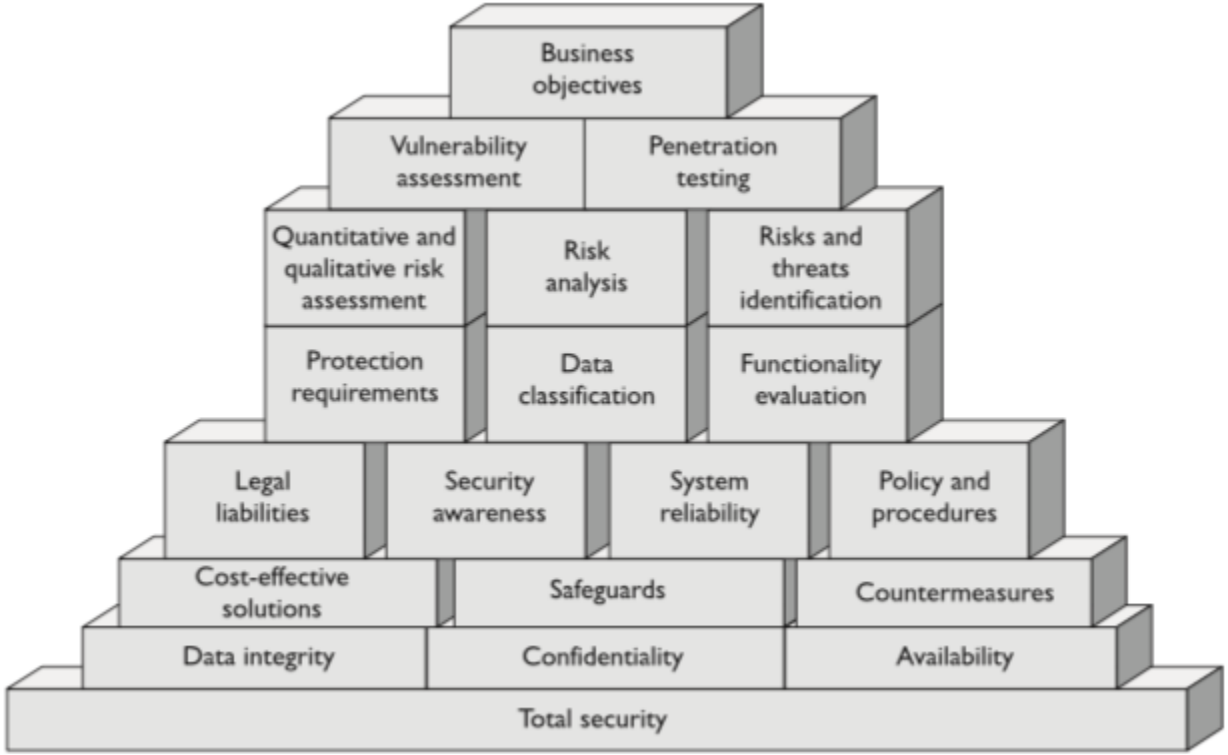
System Security Group | Lancaster University




- Risk Management is organisational control to risk
  - Risk Assessment is Identification, Analysis and Evaluation
    - Risk Analysis enables comprehension of risk

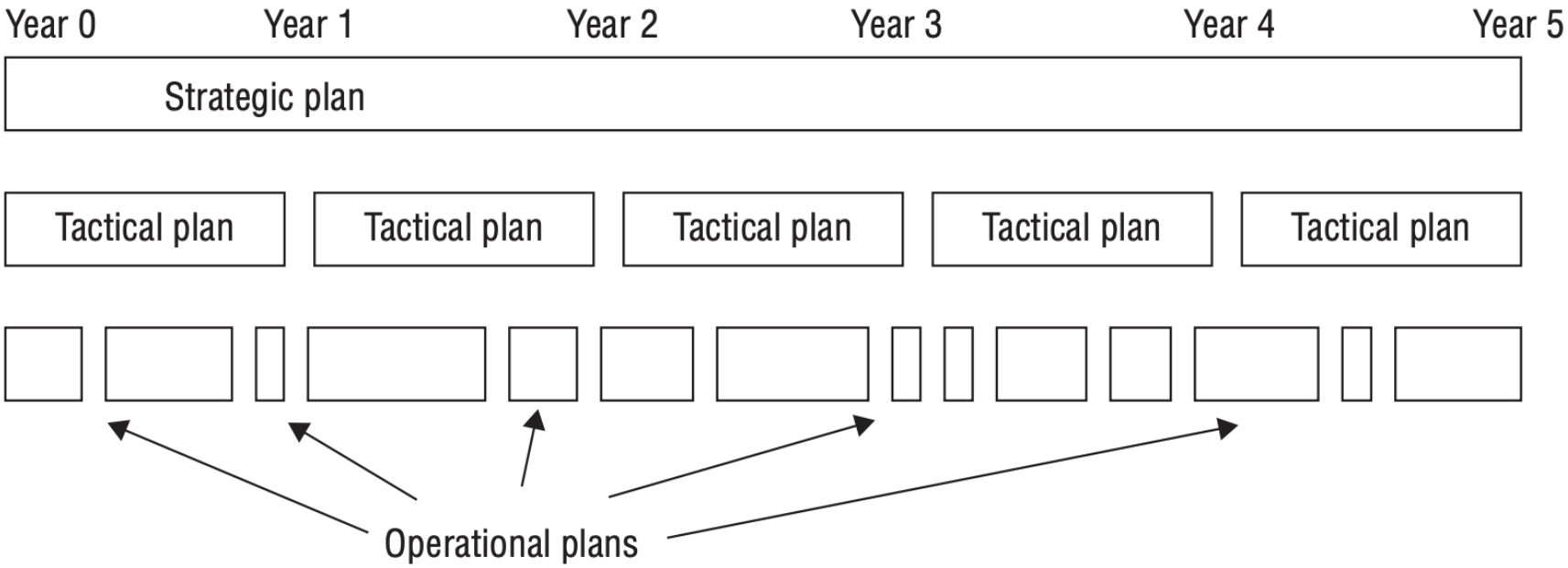
# Total Security Building Blocks





# Strategy, Tactic and Operation

System Security Group | Lancaster University



# Qualitative Assessment

- Scenarios of risk possibilities,
- Rank the seriousness  of the threats,
- Validity of countermeasures.
- Relies in judgement, best practices, intuition, experience.
- Techniques:
  - Delphi,
  - Brainstorming,
  - Storyboarding,
  - Focus groups,
  - Surveys

# Quantitative Risk Assessment/Analysis



- Attempt to assign meaningful numbers against e.g.: Safeguard costs, asset value, business impact, threat frequency, safeguard effectiveness, exploit probabilities, etc…
- Attempt to assign meaningful percentages against probability of likelihood.

# CISSP Example Risk Analysis Steps



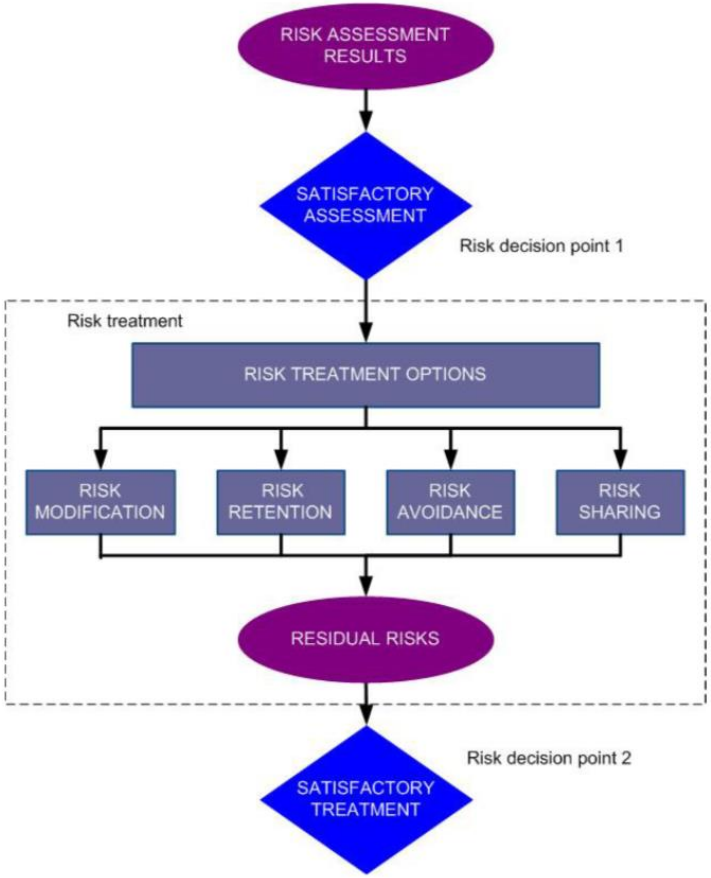
1. Identify assets and their value
2. Estimate potential loss per threat
3. Perform Threat analysis, calculate ARO
4. Derive the ALE per threat
5. Reduce, Transfer, Avoid or Accept the Risk

# Exposure and Loss Expectancy

System Security Group | Lancaster University

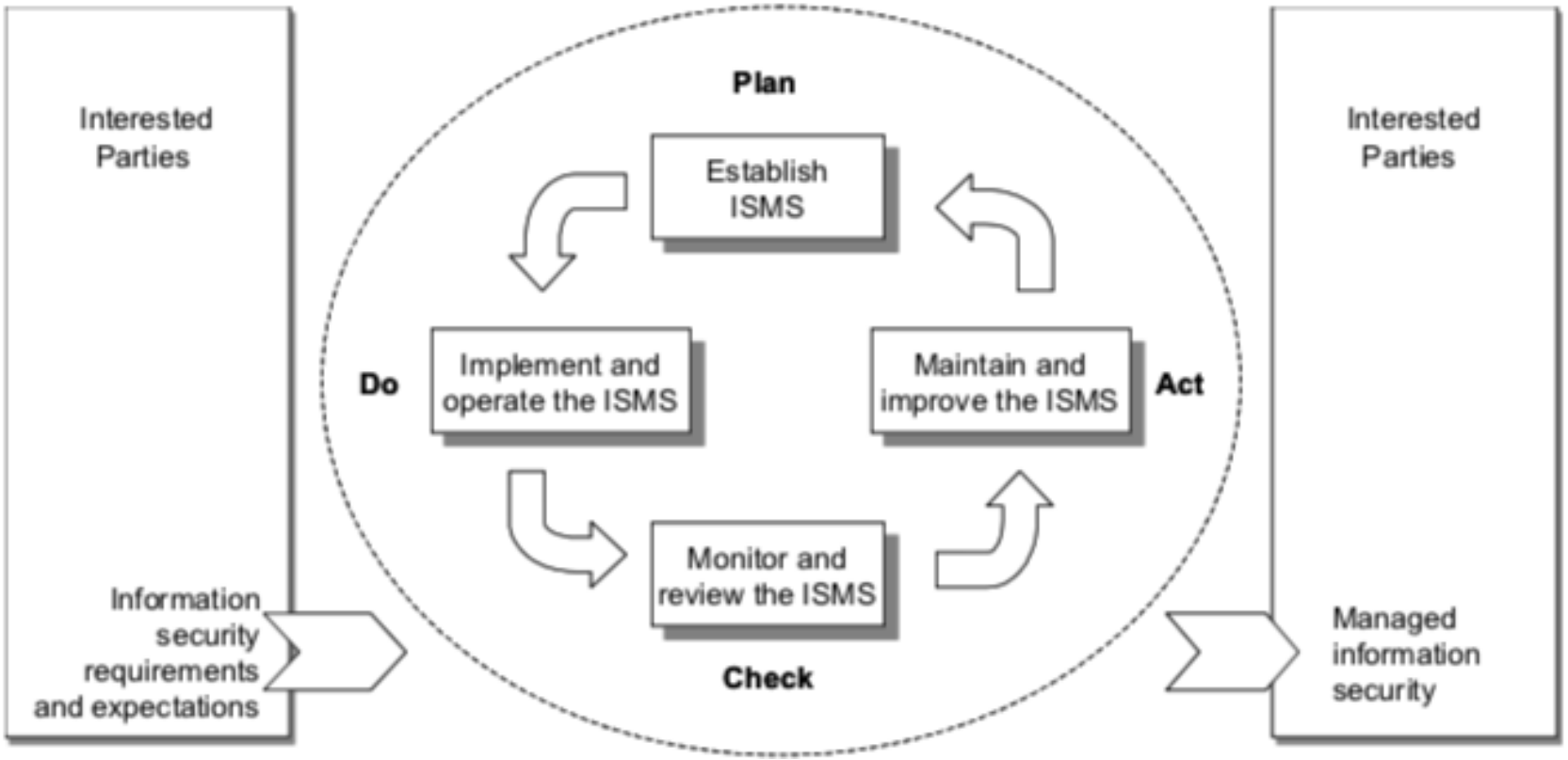

- Annual Rate of Occurrence x Single Loss Expectance
  - 10% x £550,000 = £55,000

# Risk Treatment



# Security Controls

# Plan Do Check Act



# Residual Risk

# Incident Management

# Questions?

# References


- Harris, S. (2010). CISSP All-in-One Exam Guide (5th ed.). New York: McGraw-Hill.
- https://mrcissp.com/2019/01/09/cia-triad-in-details-looks-simple-but-actually-complex/
- Chapple, M., Stewart, J.M. and Gibson, D., 2018. (ISC) 2 CISSP Certified Information Systems Security Professional Official Study Guide. New York: John Wiley & Sons
- British Standards Institute. (2005). BS ISO/IEC 27001 - Information Technology - Security Techniques – Information Security Management Systems - Requirements. Retrieved from https://bsol.bsigroup.com/Search/Search?searchKey=27001
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf
- British Standards Institute. (2011). BS ISO/IEC 27005 - Information Technology - Security Techniques – Information Security Risk Management. Retrieved from https://bsol.bsigroup.com/Search/Search?searchKey=27005
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
- https://www.ncsc.gov.uk/collection/risk-management-collection?curPage=/collection/risk-management-collection/essential-topics/fundamentals