1. Define Scope
- Define system boundaries, interfaces and dependencies
- Identify critical assets and attackers

2. Threat Analysis
- Identify threats
- Rate impact

3. Attack Analysis
- Identify attack paths
- Rate attack feasibility

4. Risk Assessment
- Evaluate risk levels

5. Risk Treatment
- Develop and prioritise risk treatment options

6. Documentation and Reporting
- Document process and findings