What is inside the ISO/IEC 27k

The code of practice (ISO/IEC 27002)

- List of 133 candidate control objectives and controls
- Each control must be addressed one by one in the evaluation plan (extras can be added)

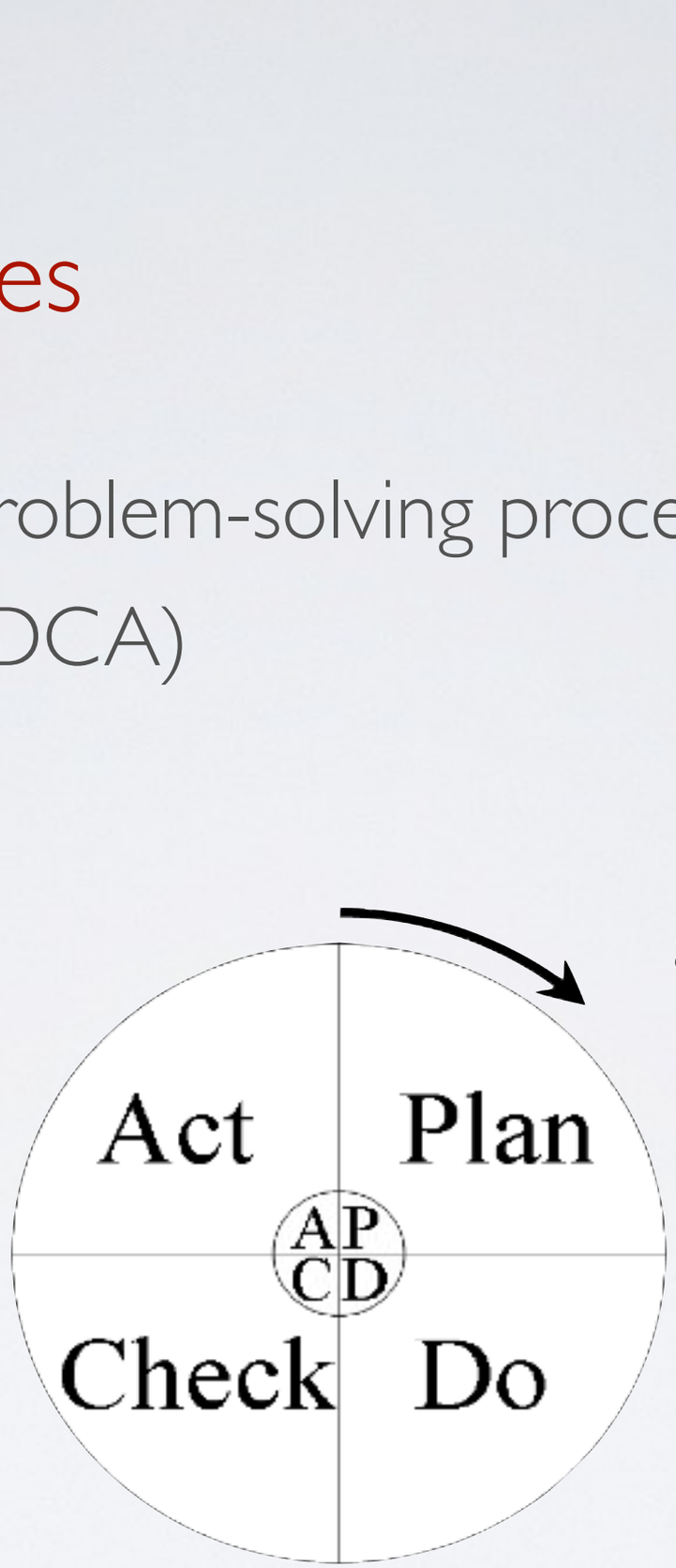
Governing principles

Based on an iterative problem-solving process

➡ Deming's Wheel (PDCA)

improve
the security assurance

run a risk analysis
and define the security policy



measure
the security solutions

design and build
security solutions
(called controls)