F. IT controls maturity assessment methodology

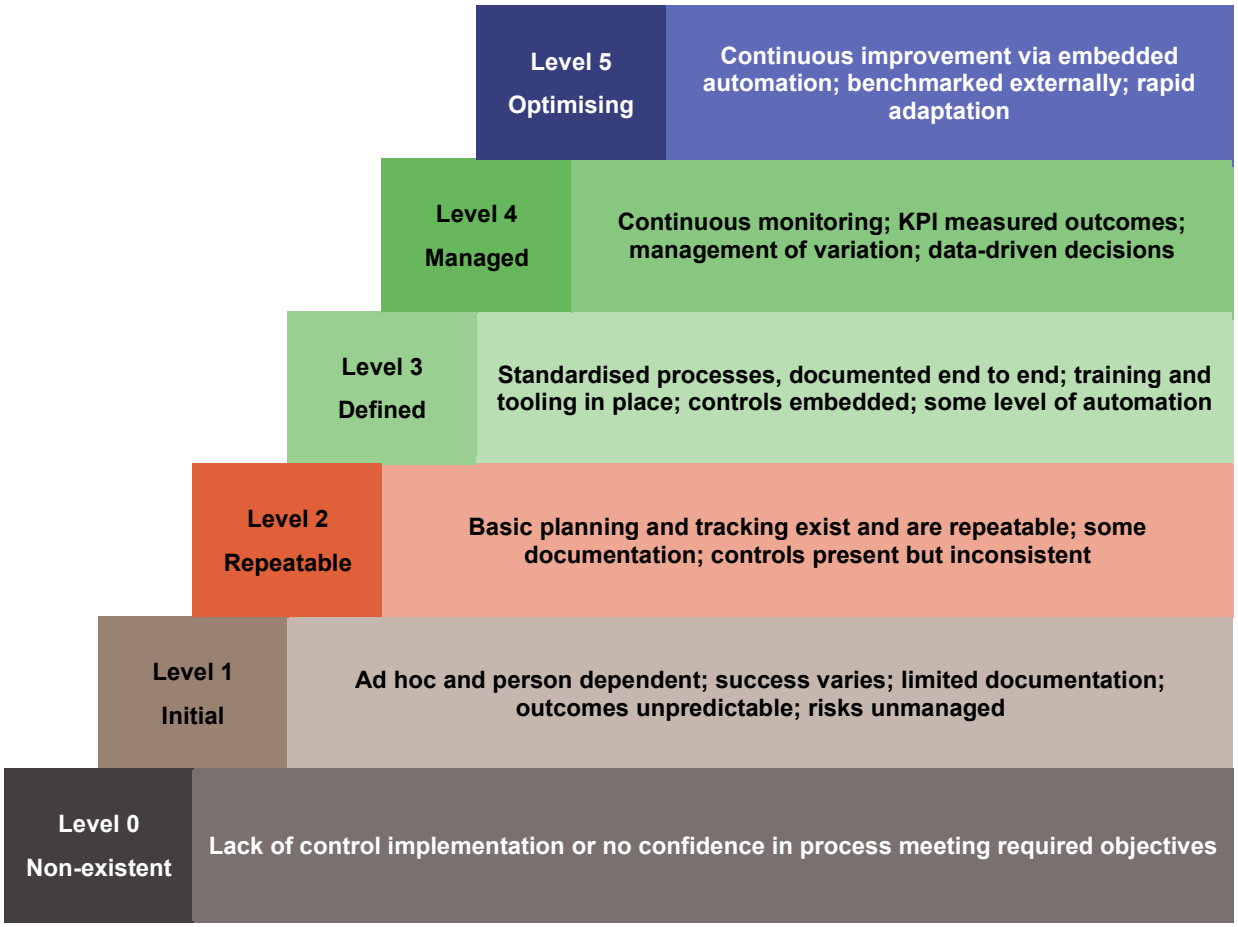
Our information technology (IT) controls maturity assessment methodology utilises the 5-level Capability Maturity Model (CMM) framework devised at Carnegie Mellon University in 1987.

The framework was originally designed to evaluate and improve software development processes used by Department of Defence contractors in the USA.

The CMM framework is now used by numerous organisations spanning different industries to assess and monitor maturity assessment of technical and non-technical processes.

Under the framework, control categories are assessed from being largely ad hoc and reactive (Level 1 – initial) to being continuously monitored, improved, and fully automated (Level 5 – optimising).

Figure F1
Capability Maturity Model (CMM) maturity levels



Source: Developed by Queensland Audit Office from the Carnegie Mellon University CMM framework.

The target maturity level for entities is Level 2 (repeatable), which represents a baseline or minimum expected level of maturity. At Level 2, IT control processes are established, and tasks are repeatable, however, process gaps, weaknesses, or errors may exist.

Level 3 (defined) represents a higher level of organisational maturity, in which processes are defined, documented, and standardised, with minimal gaps or errors existing.

Achieving Levels 4 (quantitatively managed) or 5 (optimising) represents leading practice, with extensive measurement, automation, predictive analytics, and continuous optimisation. Levels 4 and 5 generally require significant investment in technology, specialist capability, and organisational change. For most organisations, the costs and ongoing effort required to achieve and sustain these levels are unlikely to be proportionate to the associated reduction in risk.