

## Appendix 4 – Capability Maturity Model

To rank the IT Security Processes, the following CMM rankings are used:

Initial / Ad-Hoc

Repeatable but Intuitive

Defined Process

Managed and Measurable

Optimised

### 1 – Initial / Ad-Hoc

There is evidence that the organisation has recognised that IT process issues exist and need to be addressed. There are, however, no standardised processes. Instead there are ad-hoc approaches applied on an individual or case-by-case basis. Management's approach is chaotic and there is only sporadic, inconsistent communication on issues and approaches to address them.

Examples of an Initial / Ad-Hoc IT Security process:

- The IT environment is not secure and the integrity of the environment is unknown.
- Security policies, procedures and standards are not defined or documented.

### 2 – Repeatable but Intuitive

IT processes are consistently applied, however have not been formalised. There is no formal training and communication on IT standards and responsibilities are left to the individual. Processes are repeated because the same individual performs the activities.

Examples of a Repeatable but Intuitive IT Security process:

- Roles have been defined within the IT Security process, however job description including roles and responsibilities do not exist.
- No active management of the IT Security process, security tools are not integrated.

### 3 – Defined Process

Procedures have been standardised, documented and implemented and have been communicated. Overall accountability of key processes is clear. Tools are standardised, using currently available techniques. The process is managed consistently with the defined procedures and standards. There is no pro-active monitoring of process for improvement.

Examples of a Defined IT Security process:

- Security Management processes have been defined and documented. Policies, procedures and standards have documented for all basic Security functions.
- Responsibilities for Security administration have been assigned to specific individuals. These individuals have the appropriate skills and aptitude for their assigned responsibilities.

## 4 – Managed and Measurable

Responsibilities are clear and process ownership is established. IT processes are aligned with the business and with the IT strategy. Processes are occasionally improved and best internal practices are enforced. Continuous improvement is beginning to be addressed. There is limited, primarily tactical, use of technology, based on mature techniques and enforced standard tools.

Examples of a Managed IT Security process:

- The Security Management function has the appropriate segregation of duties and reports to the appropriate level of management.
- IT Security Process responsibilities have been defined and monitored through SLAs outlining measurable indicators IT has to adhere to.

## 5 – Optimised

Processes have been refined to a level of external best practice, based on results of continuous improvement and maturity modelling with other organisations. IT is used in an extensive, integrated and optimised manner to automate the workflow and provide tools to improve quality and effectiveness. Business plans and IT plans are strategically linked, increasing the competitive advantage of the enterprise.

Examples of an Optimised IT Security process:

- Security tools are deployed that allow a single point of administration for access to IT resources.
- Security processes and controls are reviewed and assessed frequently to identify potential weaknesses and eliminate or reduce them.