

## Overview of Appendix I-V

**Appendix I** (Linking Business Goals and IT Goals) provides a global view of how generic business goals relate to IT goals, the IT processes and information criteria. There are three tables: (i) the first table maps the business goals, organized according to a balanced scorecard, to the IT goals and information criteria... this helps show, for a given generic business goal, the IT goals that typically support this goal and the COBIT information criteria that relate to the business goal; (ii) the second table maps the IT goals to COBIT's IT processes and the information criteria on which the IT goal is based; (iii) the third table provides a reverse mapping showing for each IT process the IT goals that are supported. The tables help demonstrate the scope of COBIT and the overall business relationship between COBIT and business drivers, enabling typical business goals to be mapped via IT goals to the IT processes needed to support them. The tables are based on generic goals and, therefore, should be used as a guide and tailored for a specific enterprise. To provide a link back to the information criteria used for business requirements in COBIT 3rd Edition, the tables also provide an indication of the most important information criteria supported by the business and IT goals.

**Appendix II** (Mapping IT Processes to IT Governance Focus Areas, COSO, COBIT Resources and COBIT Information Criteria) provides a mapping between the COBIT IT processes and the five IT governance focus areas, the components of COSO, IT resources and the information criteria. The table also provides a relative importance indicator (high, medium and low) based on benchmarking via COBIT Online. This matrix demonstrates on one page and at a high level how the COBIT framework addresses IT governance and COSO requirements, and shows the relationship between IT processes and the IT resources and information criteria. P is used when there is a primary relation and S when there is only a secondary relation. No 'P' or 'S' does not mean that there is no relation, only that it is less important, or marginal. The importance values are based on a survey and the opinions of experts, and are provided only as a guide. Users should consider what processes are important within their own organisations.

**Appendix III** (Maturity Model for Internal Control) provides a generic maturity model showing the status of the internal control environment and the establishment of internal controls in an enterprise. The model provides a high-level guide to help COBIT users appreciate what is required for effective internal controls in IT and to help position their enterprise on the maturity scale.

**Appendix IV** provides details on the COBIT 4.0 primary reference material. For the earlier COBIT development and updating activities, a broad base of more than 40 international detailed IT standards, frameworks, guidelines and best practices was used to ensure the completeness of COBIT in addressing all areas of IT governance and control. Because COBIT is focused on *what* is required to achieve adequate management and control of IT, it is positioned at a high level. The more detailed IT standards and best practices are at a lower level of detail describing *how* to manage and control specific aspects of IT. COBIT acts as an integrator of these different guidance materials, summarising key objectives under one umbrella framework that also links to governance and business requirements. For this COBIT update (COBIT 4.0), six of the major global IT-related standards, frameworks and practices were focused on as the major supporting references to ensure appropriate coverage, consistency and alignment. These are: (i) Committee of Sponsoring Organisations of the Treadway Commission (COSO) Internal Control—Integrated Framework, 1994 and Enterprise Risk Management—Integrated Framework, 2004; (ii) Office of Government Commerce (OGC®) IT Infrastructure Library® (ITIL®), 1999-2004; (iii) International Organisation for Standardisation ISO/IEC 17799:2005, Code of Practice for Information Security Management; (iv) Software Engineering Institute (SEI®) SEI Capability Maturity Model (CMM®), 1993 and SEI Capability Maturity Model Integration (CMMI®), 2000; (v) Project Management Institute (PMI®) Project Management Body of Knowledge (PMBOK®), 2000; (vi) Information Security Forum (ISF) The Standard of Good Practice for Information Security, 2003.

**Appendix V** provides cross-references between COBIT 3<sup>rd</sup> Edition and COBIT 4.0. Related headings in this appendix include: Framework-level changes, Detailed Control Objectives, and Management Guidelines. The latter is followed by the actual cross-references between the noted versions of COBIT.