ISACA®

Trust in, and value from, information systems

San Francisco Chapter

G32

The Changing Influences of Social Media, WikiLeaks and Whistleblowers

A Modest Proposal: The Future of IT Auditing

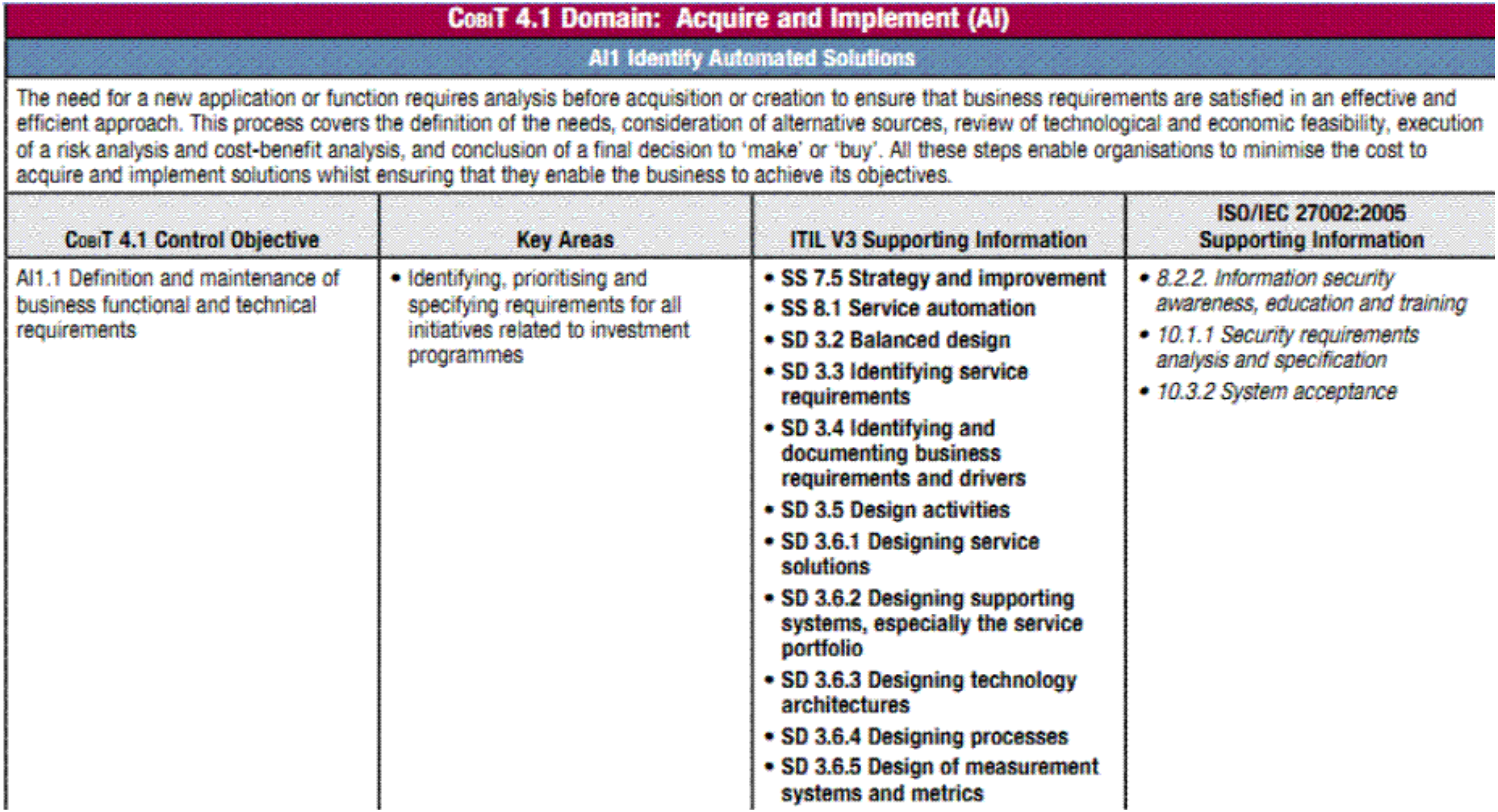
by

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives

- AI (Acquire & Implement)
  - 1, 2, 3 & 4 --- 6 & 7
- DS (Deliver & Support)
  - 3, 4, & 5 --- 8, 9, 10, 11, 12 & 13
- ME (Monitor & Evaluate)
  - 1 & 2
- PO (Plan & Organize)
  - 1, 2, & 3 --- 5 & 6 --- 8, 9, & 10

Mapping ITIL V3 & ISO/IEC 27002 W/CobiT 4.1 Control Objectives: Acquire and Implement (AI)



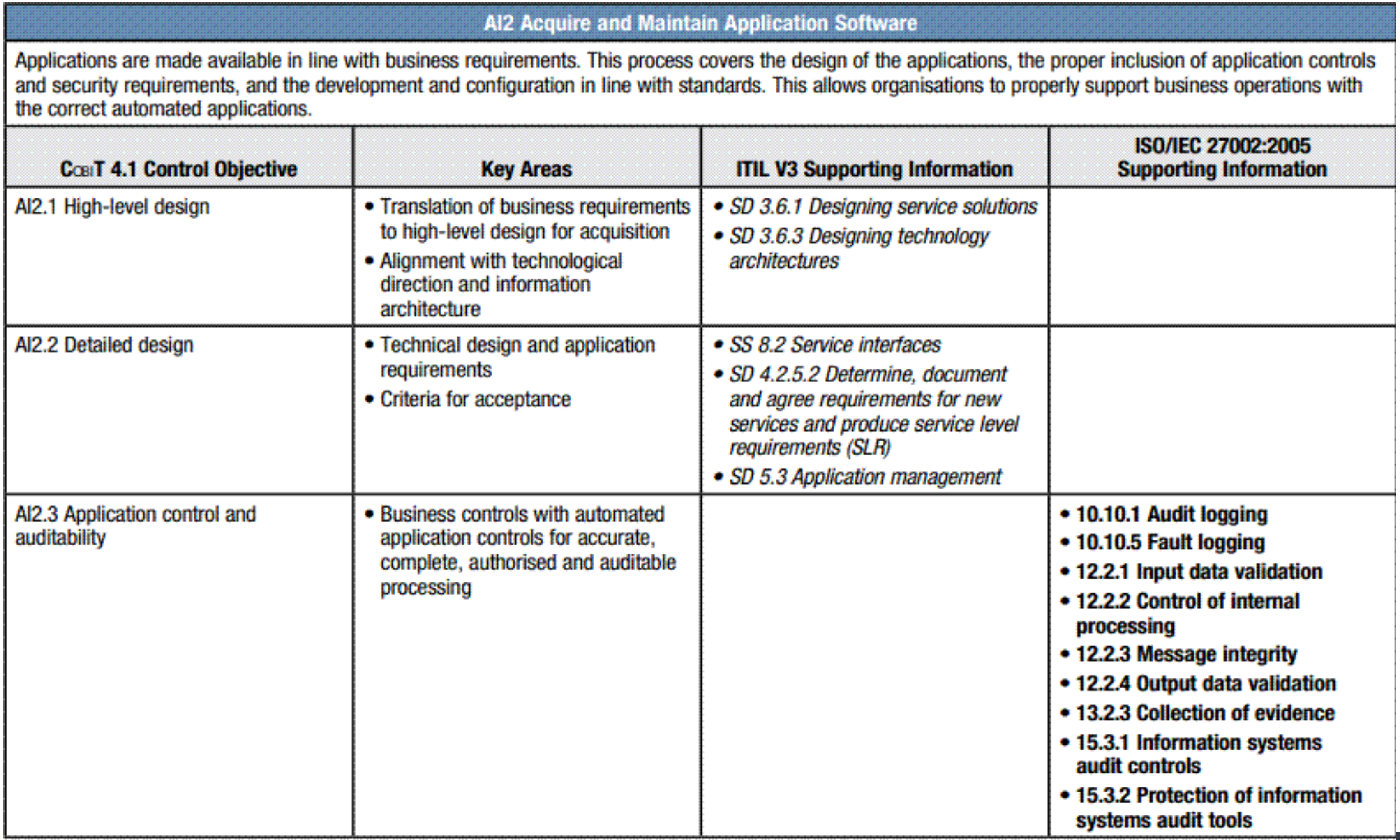
CobiT 4.1 Domain: Acquire and Implement (AI)

AI1 Identify Automated Solutions

The need for a new application or function requires analysis before acquisition or creation to ensure that business requirements are satisfied in an effective and efficient approach. This process covers the definition of the needs, consideration of alternative sources, review of technological and economic feasibility, execution of a risk analysis and cost-benefit analysis, and conclusion of a final decision to 'make' or 'buy'. All these steps enable organisations to minimise the cost to acquire and implement solutions whilst ensuring that they enable the business to achieve its objectives.

CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
AI1.1 Definition and maintenance of business functional and technical requirements	• Identifying, prioritising and specifying requirements for all initiatives related to investment programmes	• SS 7.5 Strategy and improvement • SS 8.1 Service automation • SD 3.2 Balanced design • SD 3.3 Identifying service requirements • SD 3.4 Identifying and documenting business requirements and drivers • SD 3.5 Design activities • SD 3.6.1 Designing service solutions • SD 3.6.2 Designing supporting systems, especially the service portfolio • SD 3.6.3 Designing technology architectures • SD 3.6.4 Designing processes • SD 3.6.5 Design of measurement systems and metrics	• *8.2.2. Information security awareness, education and training* • *10.1.1 Security requirements analysis and specification* • *10.3.2 System acceptance*

Mapping ITIL V3 & ISO/IEC 27002 W/CobiT 4.1 Control Objectives: Acquire and Implement (AI)

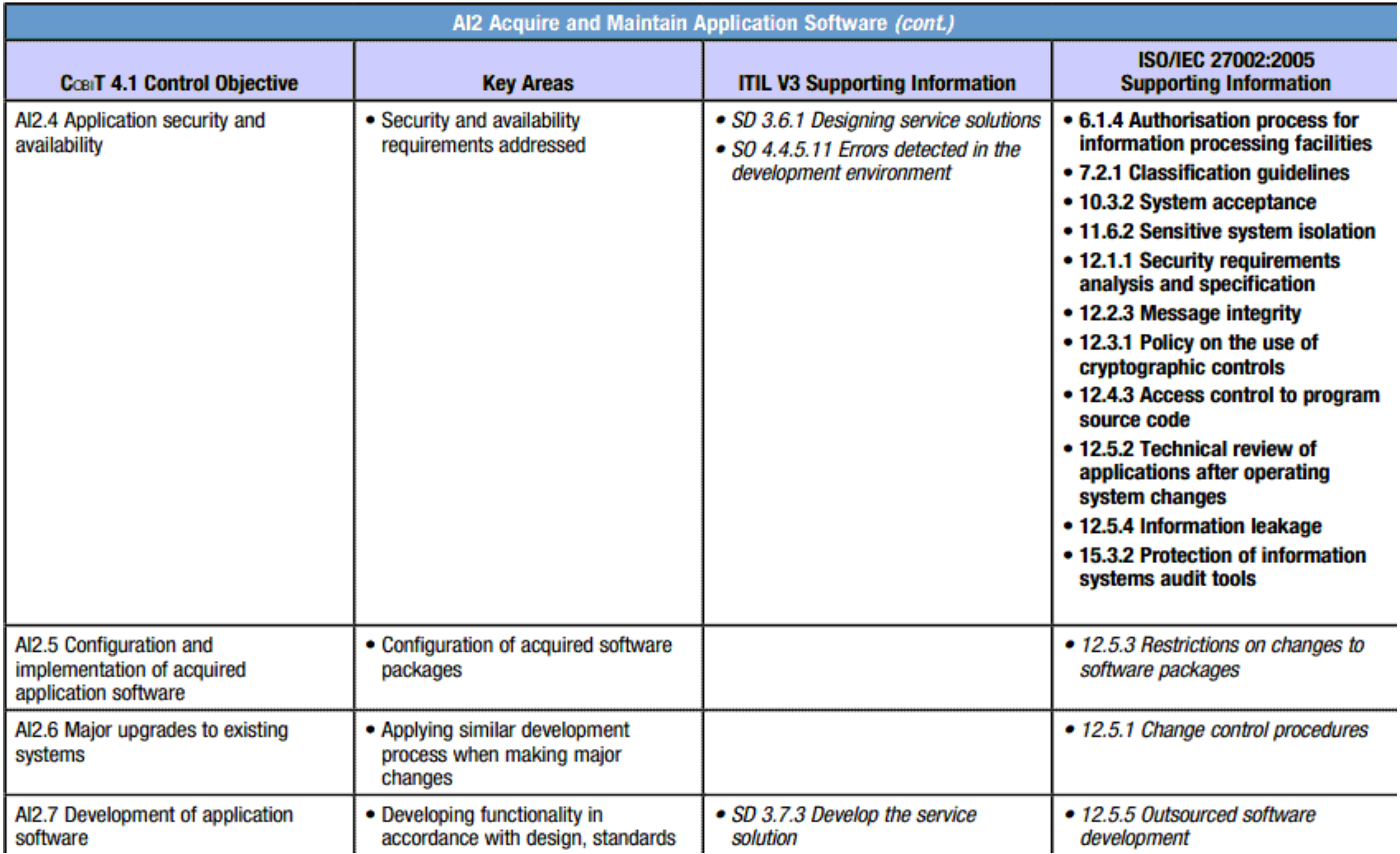


AI2 Acquire and Maintain Application Software

Applications are made available in line with business requirements. This process covers the design of the applications, the proper inclusion of application controls and security requirements, and the development and configuration in line with standards. This allows organisations to properly support business operations with the correct automated applications.

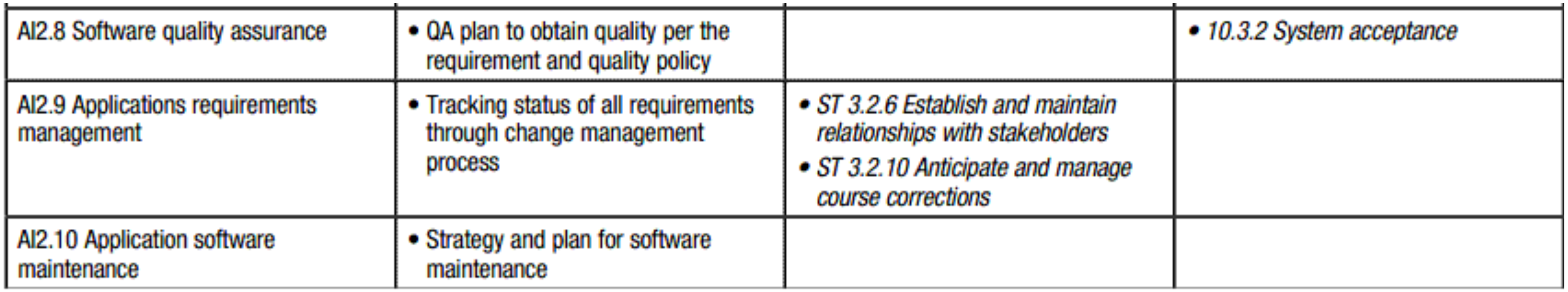
CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
AI2.1 High-level design	• Translation of business requirements to high-level design for acquisition • Alignment with technological direction and information architecture	• *SD 3.6.1 Designing service solutions* • *SD 3.6.3 Designing technology architectures*	
AI2.2 Detailed design	• Technical design and application requirements • Criteria for acceptance	• *SS 8.2 Service interfaces* • *SD 4.2.5.2 Determine, document and agree requirements for new services and produce service level requirements (SLR)* • *SD 5.3 Application management*	
AI2.3 Application control and auditability	• Business controls with automated application controls for accurate, complete, authorised and auditable processing		• **10.10.1 Audit logging** • **10.10.5 Fault logging** • **12.2.1 Input data validation** • **12.2.2 Control of internal processing** • **12.2.3 Message integrity** • **12.2.4 Output data validation** • **13.2.3 Collection of evidence** • **15.3.1 Information systems audit controls** • **15.3.2 Protection of information systems audit tools**

Mapping ITIL V3 & ISO/IEC 27002 W/CobiT 4.1 Control Objectives: Acquire and Implement (AI)



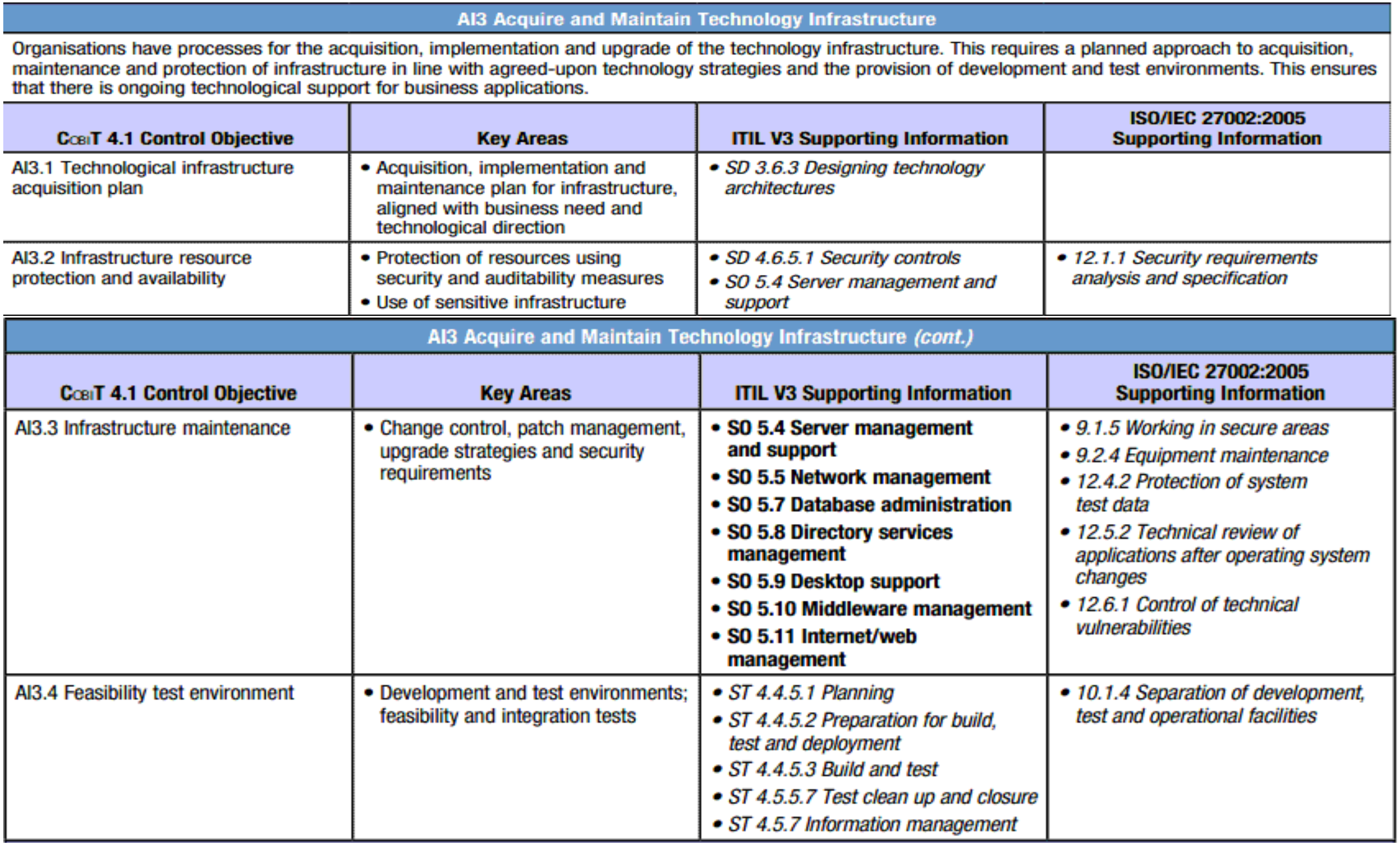
AI2 Acquire and Maintain Application Software *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
AI2.4 Application security and availability	• Security and availability requirements addressed	• *SD 3.6.1 Designing service solutions* • *SO 4.4.5.11 Errors detected in the development environment*	• **6.1.4 Authorisation process for information processing facilities** • **7.2.1 Classification guidelines** • **10.3.2 System acceptance** • **11.6.2 Sensitive system isolation** • **12.1.1 Security requirements analysis and specification** • **12.2.3 Message integrity** • **12.3.1 Policy on the use of cryptographic controls** • **12.4.3 Access control to program source code** • **12.5.2 Technical review of applications after operating system changes** • **12.5.4 Information leakage** • **15.3.2 Protection of information systems audit tools**
AI2.5 Configuration and implementation of acquired application software	• Configuration of acquired software packages		• *12.5.3 Restrictions on changes to software packages*
AI2.6 Major upgrades to existing systems	• Applying similar development process when making major changes		• *12.5.1 Change control procedures*
AI2.7 Development of application software	• Developing functionality in accordance with design, standards	• *SD 3.7.3 Develop the service solution*	• *12.5.5 Outsourced software development*

Mapping ITIL V3 & ISO/IEC 27002 W/CobiT 4.1 Control Objectives: Acquire and Implement (AI)



AI2.8 Software quality assurance	• QA plan to obtain quality per the requirement and quality policy		• *10.3.2 System acceptance*
AI2.9 Applications requirements management	• Tracking status of all requirements through change management process	• *ST 3.2.6 Establish and maintain relationships with stakeholders* • *ST 3.2.10 Anticipate and manage course corrections*	
AI2.10 Application software maintenance	• Strategy and plan for software maintenance		

Mapping ITIL V3 & ISO/IEC 27002 W/CobiT 4.1 Control Objectives: Acquire and Implement (AI)

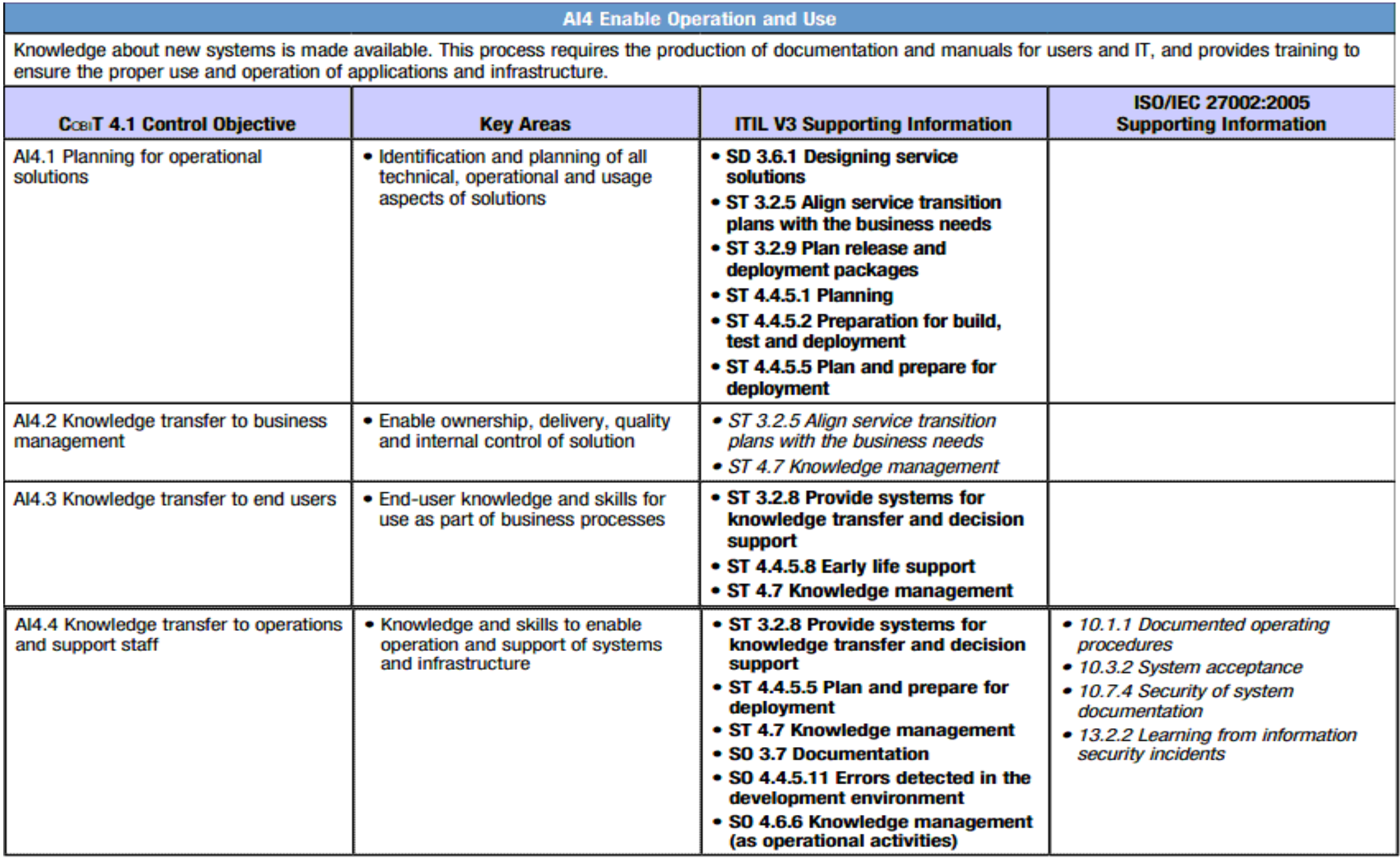


AI3 Acquire and Maintain Technology Infrastructure

Organisations have processes for the acquisition, implementation and upgrade of the technology infrastructure. This requires a planned approach to acquisition, maintenance and protection of infrastructure in line with agreed-upon technology strategies and the provision of development and test environments. This ensures that there is ongoing technological support for business applications.

CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
AI3.1 Technological infrastructure acquisition plan	• Acquisition, implementation and maintenance plan for infrastructure, aligned with business need and technological direction	• *SD 3.6.3 Designing technology architectures*	
AI3.2 Infrastructure resource protection and availability	• Protection of resources using security and auditability measures • Use of sensitive infrastructure	• *SD 4.6.5.1 Security controls* • *SO 5.4 Server management and support*	• *12.1.1 Security requirements analysis and specification*
AI3.3 Infrastructure maintenance	• Change control, patch management, upgrade strategies and security requirements	• **SO 5.4 Server management and support** • **SO 5.5 Network management** • **SO 5.7 Database administration** • **SO 5.8 Directory services management** • **SO 5.9 Desktop support** • **SO 5.10 Middleware management** • **SO 5.11 Internet/web management**	• *9.1.5 Working in secure areas* • *9.2.4 Equipment maintenance* • *12.4.2 Protection of system test data* • *12.5.2 Technical review of applications after operating system changes* • *12.6.1 Control of technical vulnerabilities*
AI3.4 Feasibility test environment	• Development and test environments; feasibility and integration tests	• *ST 4.4.5.1 Planning* • *ST 4.4.5.2 Preparation for build, test and deployment* • *ST 4.4.5.3 Build and test* • *ST 4.5.5.7 Test clean up and closure* • *ST 4.5.7 Information management*	• *10.1.4 Separation of development, test and operational facilities*

Mapping ITIL V3 & ISO/IEC 27002 W/CobiT 4.1 Control Objectives: Acquire and Implement (AI)

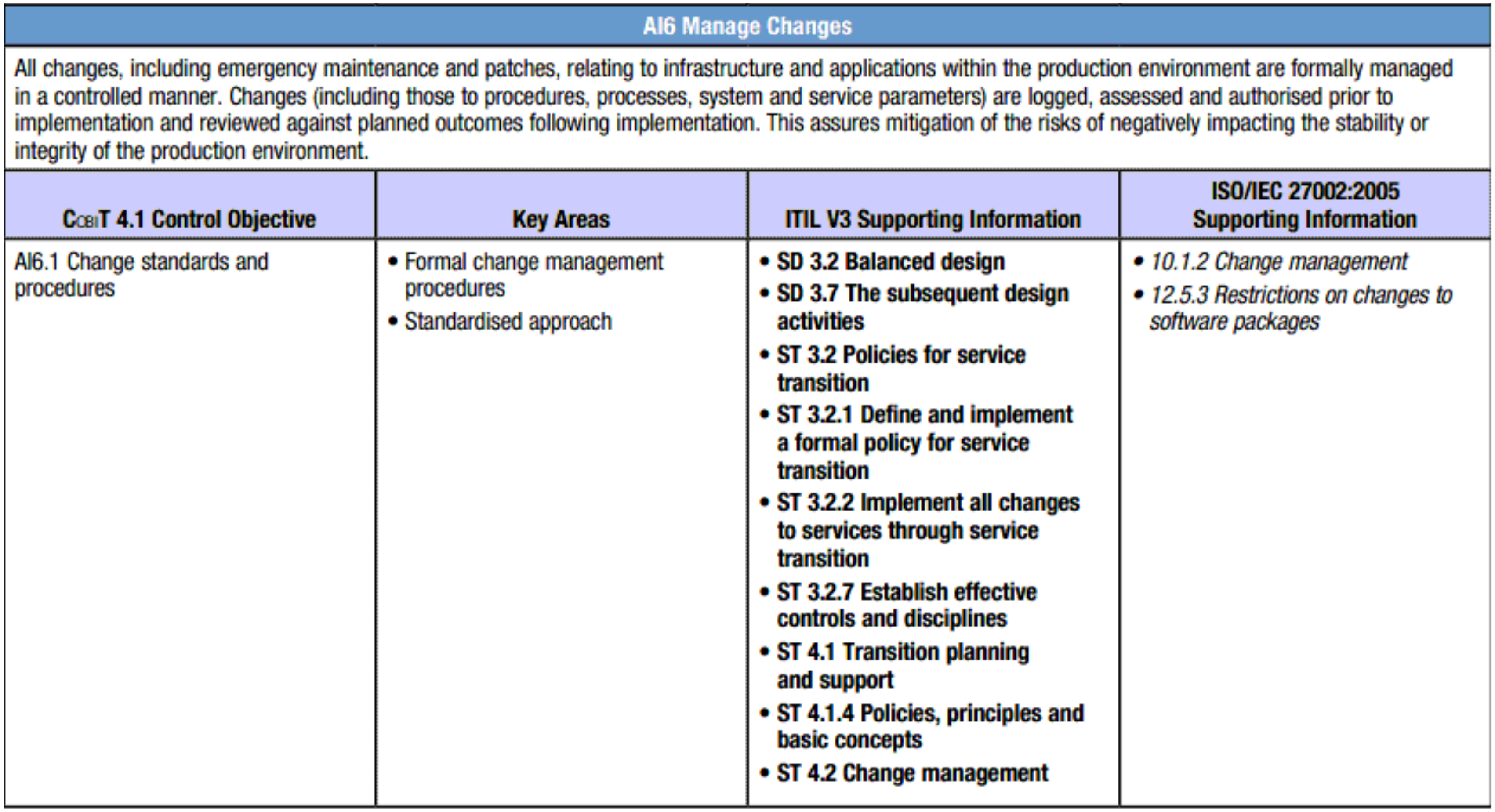


AI4 Enable Operation and Use

Knowledge about new systems is made available. This process requires the production of documentation and manuals for users and IT, and provides training to ensure the proper use and operation of applications and infrastructure.

CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
AI4.1 Planning for operational solutions	• Identification and planning of all technical, operational and usage aspects of solutions	• **SD 3.6.1 Designing service solutions** • **ST 3.2.5 Align service transition plans with the business needs** • **ST 3.2.9 Plan release and deployment packages** • **ST 4.4.5.1 Planning** • **ST 4.4.5.2 Preparation for build, test and deployment** • **ST 4.4.5.5 Plan and prepare for deployment**	
AI4.2 Knowledge transfer to business management	• Enable ownership, delivery, quality and internal control of solution	• *ST 3.2.5 Align service transition plans with the business needs* • *ST 4.7 Knowledge management*	
AI4.3 Knowledge transfer to end users	• End-user knowledge and skills for use as part of business processes	• **ST 3.2.8 Provide systems for knowledge transfer and decision support** • **ST 4.4.5.8 Early life support** • **ST 4.7 Knowledge management**	
AI4.4 Knowledge transfer to operations and support staff	• Knowledge and skills to enable operation and support of systems and infrastructure	• **ST 3.2.8 Provide systems for knowledge transfer and decision support** • **ST 4.4.5.5 Plan and prepare for deployment** • **ST 4.7 Knowledge management** • **SO 3.7 Documentation** • **SO 4.4.5.11 Errors detected in the development environment** • **SO 4.6.6 Knowledge management (as operational activities)**	• *10.1.1 Documented operating procedures* • *10.3.2 System acceptance* • *10.7.4 Security of system documentation* • *13.2.2 Learning from information security incidents*

Mapping ITIL V3 & ISO/IEC 27002 W/CobiT 4.1 Control Objectives: Acquire and Implement (AI)

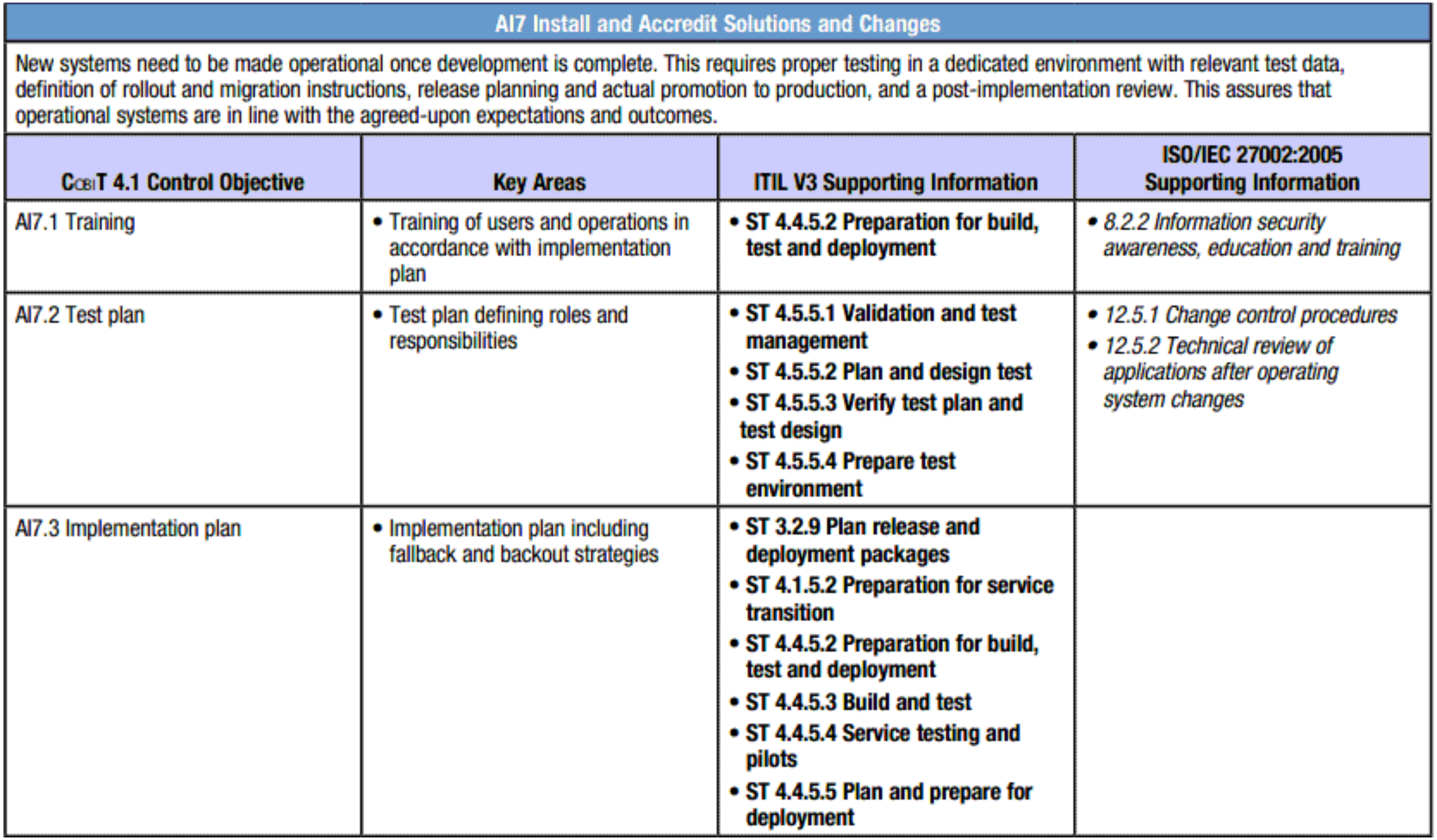


AI6 Manage Changes

All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment are formally managed in a controlled manner. Changes (including those to procedures, processes, system and service parameters) are logged, assessed and authorised prior to implementation and reviewed against planned outcomes following implementation. This assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.

CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
AI6.1 Change standards and procedures	• Formal change management procedures • Standardised approach	• **SD 3.2 Balanced design** • **SD 3.7 The subsequent design activities** • **ST 3.2 Policies for service transition** • **ST 3.2.1 Define and implement a formal policy for service transition** • **ST 3.2.2 Implement all changes to services through service transition** • **ST 3.2.7 Establish effective controls and disciplines** • **ST 4.1 Transition planning and support** • **ST 4.1.4 Policies, principles and basic concepts** • **ST 4.2 Change management**	• *10.1.2 Change management* • *12.5.3 Restrictions on changes to software packages*

Mapping ITIL V3 & ISO/IEC 27002 W/CobiT 4.1 Control Objectives: Acquire and Implement (AI)

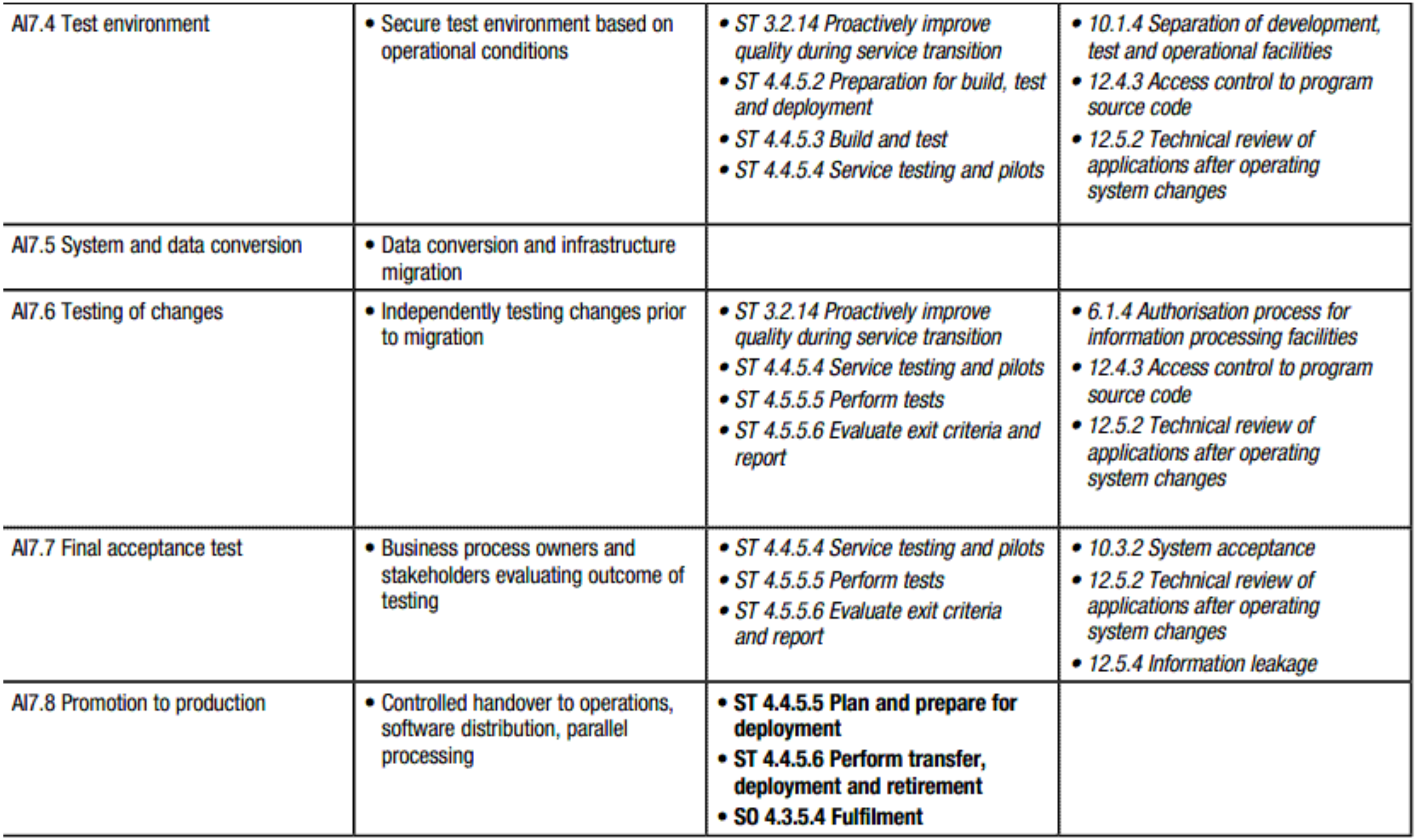


AI7 Install and Accredit Solutions and Changes

New systems need to be made operational once development is complete. This requires proper testing in a dedicated environment with relevant test data, definition of rollout and migration instructions, release planning and actual promotion to production, and a post-implementation review. This assures that operational systems are in line with the agreed-upon expectations and outcomes.

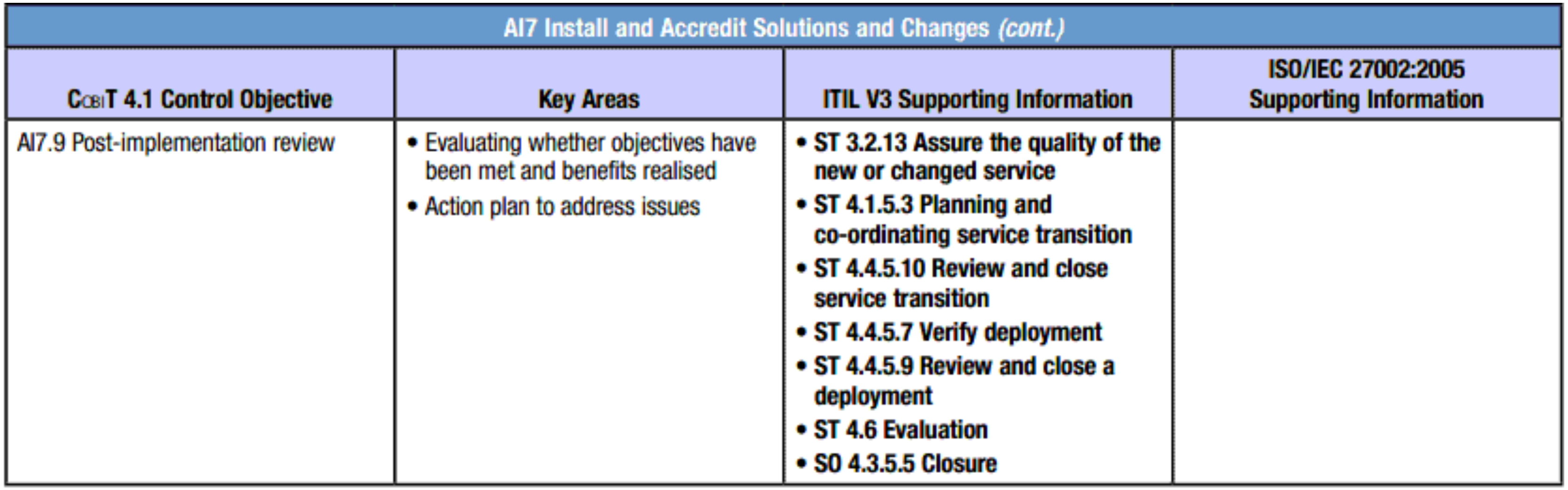
CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
AI7.1 Training	• Training of users and operations in accordance with implementation plan	• **ST 4.4.5.2 Preparation for build, test and deployment**	• *8.2.2 Information security awareness, education and training*
AI7.2 Test plan	• Test plan defining roles and responsibilities	• **ST 4.5.5.1 Validation and test management** • **ST 4.5.5.2 Plan and design test** • **ST 4.5.5.3 Verify test plan and test design** • **ST 4.5.5.4 Prepare test environment**	• *12.5.1 Change control procedures* • *12.5.2 Technical review of applications after operating system changes*
AI7.3 Implementation plan	• Implementation plan including fallback and backout strategies	• **ST 3.2.9 Plan release and deployment packages** • **ST 4.1.5.2 Preparation for service transition** • **ST 4.4.5.2 Preparation for build, test and deployment** • **ST 4.4.5.3 Build and test** • **ST 4.4.5.4 Service testing and pilots** • **ST 4.4.5.5 Plan and prepare for deployment**	

Mapping ITIL V3 & ISO/IEC 27002 W/CobiT 4.1 Control Objectives: Acquire and Implement (AI)



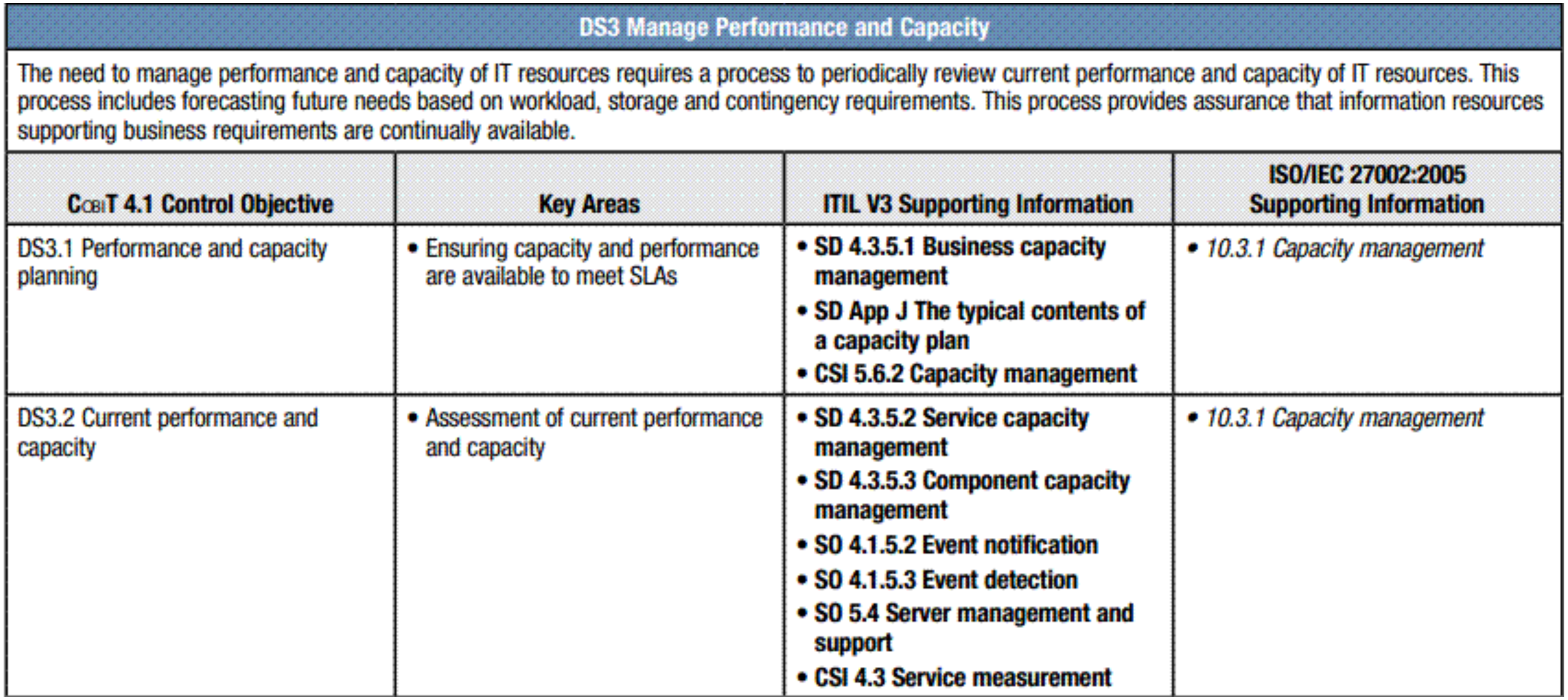
AI7.4 Test environment	• Secure test environment based on operational conditions	• *ST 3.2.14 Proactively improve quality during service transition* • *ST 4.4.5.2 Preparation for build, test and deployment* • *ST 4.4.5.3 Build and test* • *ST 4.4.5.4 Service testing and pilots*	• *10.1.4 Separation of development, test and operational facilities* • *12.4.3 Access control to program source code* • *12.5.2 Technical review of applications after operating system changes*
AI7.5 System and data conversion	• Data conversion and infrastructure migration		
AI7.6 Testing of changes	• Independently testing changes prior to migration	• *ST 3.2.14 Proactively improve quality during service transition* • *ST 4.4.5.4 Service testing and pilots* • *ST 4.5.5.5 Perform tests* • *ST 4.5.5.6 Evaluate exit criteria and report*	• *6.1.4 Authorisation process for information processing facilities* • *12.4.3 Access control to program source code* • *12.5.2 Technical review of applications after operating system changes*
AI7.7 Final acceptance test	• Business process owners and stakeholders evaluating outcome of testing	• *ST 4.4.5.4 Service testing and pilots* • *ST 4.5.5.5 Perform tests* • *ST 4.5.5.6 Evaluate exit criteria and report*	• *10.3.2 System acceptance* • *12.5.2 Technical review of applications after operating system changes* • *12.5.4 Information leakage*
AI7.8 Promotion to production	• Controlled handover to operations, software distribution, parallel processing	• **ST 4.4.5.5 Plan and prepare for deployment** • **ST 4.4.5.6 Perform transfer, deployment and retirement** • **SO 4.3.5.4 Fulfilment**	

Mapping ITIL V3 & ISO/IEC 27002 W/CobiT 4.1 Control Objectives: Acquire and Implement (AI)



AI7 Install and Accredit Solutions and Changes *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
AI7.9 Post-implementation review	• Evaluating whether objectives have been met and benefits realised • Action plan to address issues	• **ST 3.2.13 Assure the quality of the new or changed service** • **ST 4.1.5.3 Planning and co-ordinating service transition** • **ST 4.4.5.10 Review and close service transition** • **ST 4.4.5.7 Verify deployment** • **ST 4.4.5.9 Review and close a deployment** • **ST 4.6 Evaluation** • **SO 4.3.5.5 Closure**	

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Deliver and Support (DS)

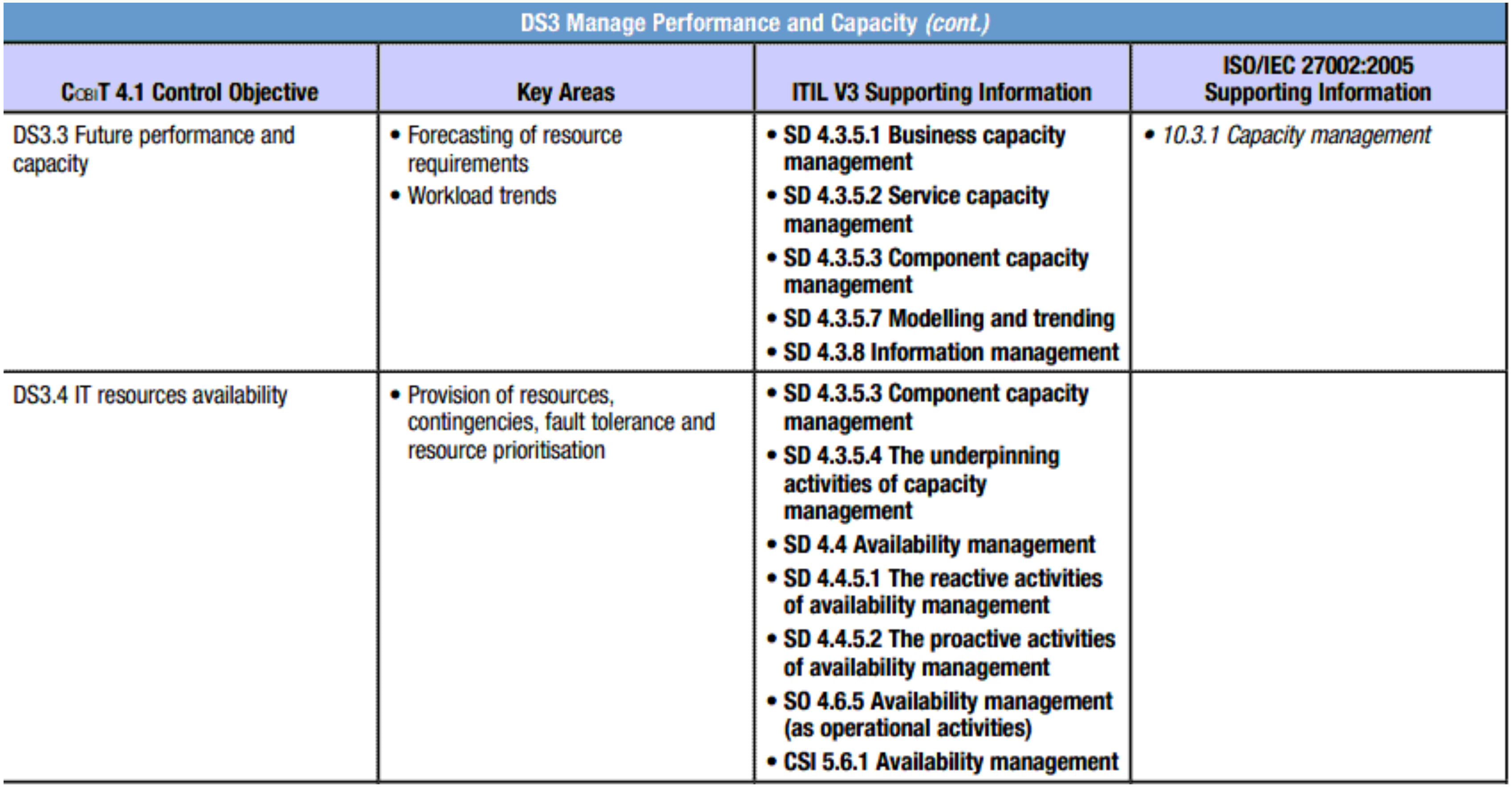


DS3 Manage Performance and Capacity

The need to manage performance and capacity of IT resources requires a process to periodically review current performance and capacity of IT resources. This process includes forecasting future needs based on workload, storage and contingency requirements. This process provides assurance that information resources supporting business requirements are continually available.

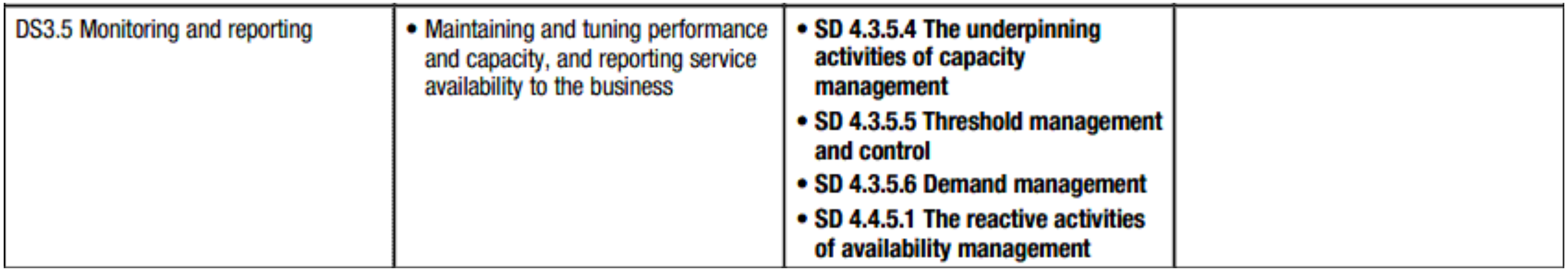
CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS3.1 Performance and capacity planning	• Ensuring capacity and performance are available to meet SLAs	• **SD 4.3.5.1 Business capacity management** • **SD App J The typical contents of a capacity plan** • **CSI 5.6.2 Capacity management**	• *10.3.1 Capacity management*
DS3.2 Current performance and capacity	• Assessment of current performance and capacity	• **SD 4.3.5.2 Service capacity management** • **SD 4.3.5.3 Component capacity management** • **SO 4.1.5.2 Event notification** • **SO 4.1.5.3 Event detection** • **SO 5.4 Server management and support** • **CSI 4.3 Service measurement**	• *10.3.1 Capacity management*

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Deliver and Support (DS)



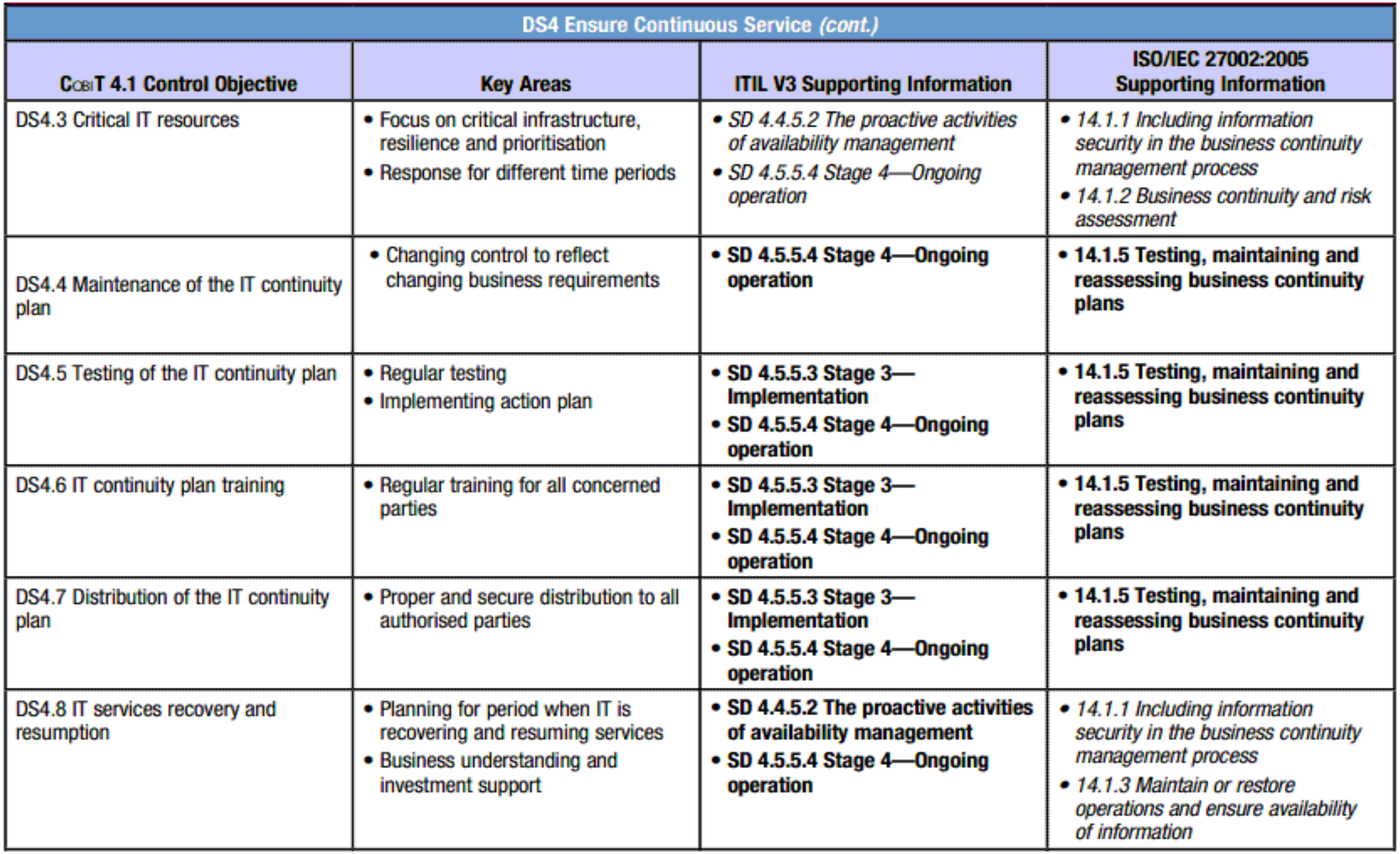
DS3 Manage Performance and Capacity *(cont.)*			
CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS3.3 Future performance and capacity	• Forecasting of resource requirements • Workload trends	• **SD 4.3.5.1 Business capacity management** • **SD 4.3.5.2 Service capacity management** • **SD 4.3.5.3 Component capacity management** • **SD 4.3.5.7 Modelling and trending** • **SD 4.3.8 Information management**	• *10.3.1 Capacity management*
DS3.4 IT resources availability	• Provision of resources, contingencies, fault tolerance and resource prioritisation	• **SD 4.3.5.3 Component capacity management** • **SD 4.3.5.4 The underpinning activities of capacity management** • **SD 4.4 Availability management** • **SD 4.4.5.1 The reactive activities of availability management** • **SD 4.4.5.2 The proactive activities of availability management** • **SO 4.6.5 Availability management (as operational activities)** • **CSI 5.6.1 Availability management**	

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Deliver and Support (DS)



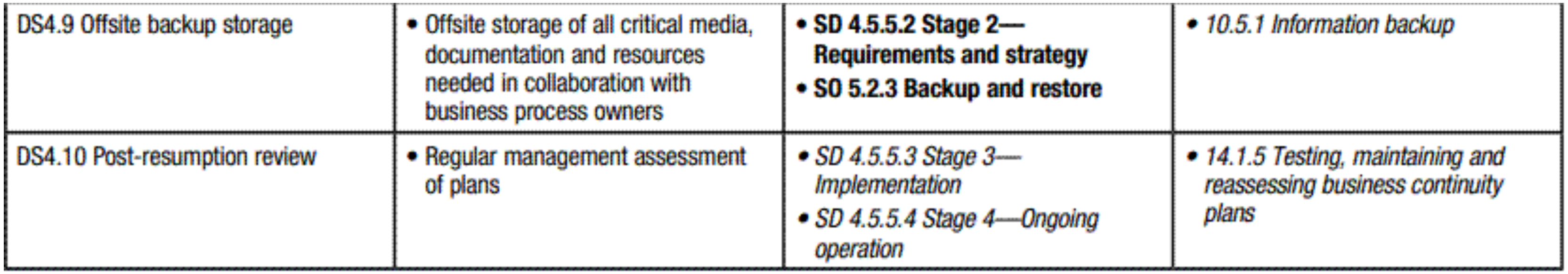
DS3.5 Monitoring and reporting	• Maintaining and tuning performance and capacity, and reporting service availability to the business	• **SD 4.3.5.4 The underpinning activities of capacity management** • **SD 4.3.5.5 Threshold management and control** • **SD 4.3.5.6 Demand management** • **SD 4.4.5.1 The reactive activities of availability management**	

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Deliver and Support (DS)



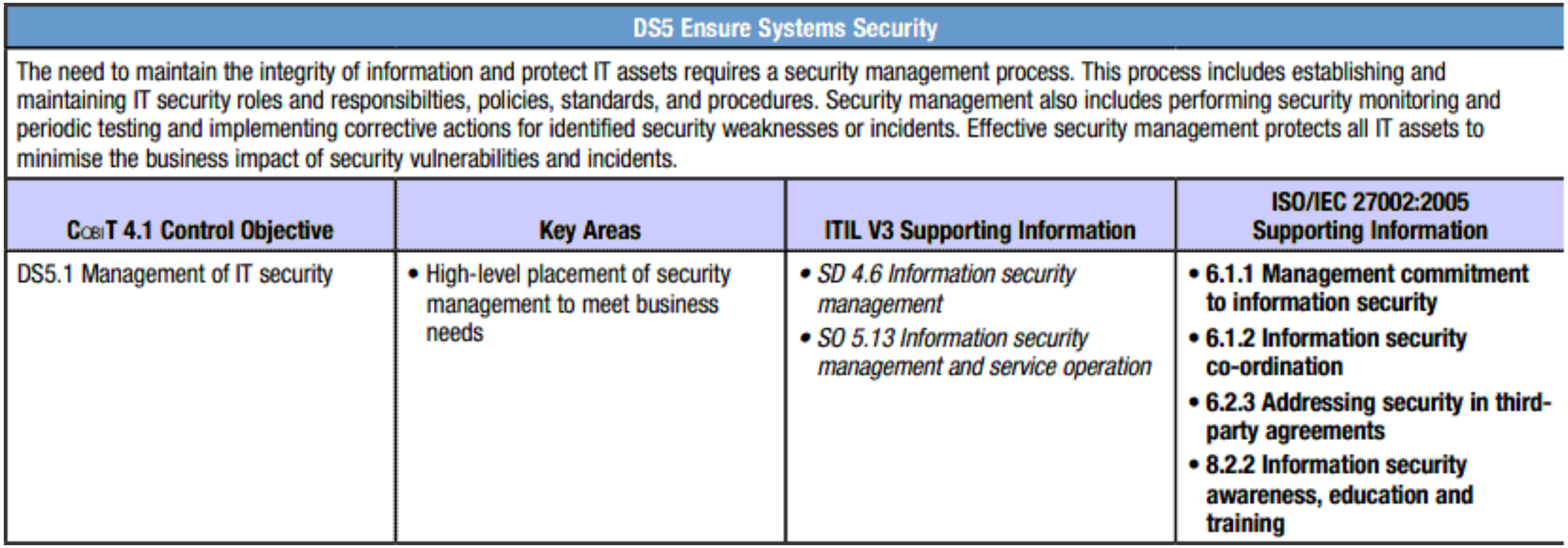
DS4 Ensure Continuous Service *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
DS4.3 Critical IT resources	• Focus on critical infrastructure, resilience and prioritisation • Response for different time periods	• *SD 4.4.5.2 The proactive activities of availability management* • *SD 4.5.5.4 Stage 4—Ongoing operation*	• *14.1.1 Including information security in the business continuity management process* • *14.1.2 Business continuity and risk assessment*
DS4.4 Maintenance of the IT continuity plan	• Changing control to reflect changing business requirements	• **SD 4.5.5.4 Stage 4—Ongoing operation**	• **14.1.5 Testing, maintaining and reassessing business continuity plans**
DS4.5 Testing of the IT continuity plan	• Regular testing • Implementing action plan	• **SD 4.5.5.3 Stage 3—Implementation** • **SD 4.5.5.4 Stage 4—Ongoing operation**	• **14.1.5 Testing, maintaining and reassessing business continuity plans**
DS4.6 IT continuity plan training	• Regular training for all concerned parties	• **SD 4.5.5.3 Stage 3—Implementation** • **SD 4.5.5.4 Stage 4—Ongoing operation**	• **14.1.5 Testing, maintaining and reassessing business continuity plans**
DS4.7 Distribution of the IT continuity plan	• Proper and secure distribution to all authorised parties	• **SD 4.5.5.3 Stage 3—Implementation** • **SD 4.5.5.4 Stage 4—Ongoing operation**	• **14.1.5 Testing, maintaining and reassessing business continuity plans**
DS4.8 IT services recovery and resumption	• Planning for period when IT is recovering and resuming services • Business understanding and investment support	• **SD 4.4.5.2 The proactive activities of availability management** • **SD 4.5.5.4 Stage 4—Ongoing operation**	• *14.1.1 Including information security in the business continuity management process* • *14.1.3 Maintain or restore operations and ensure availability of information*

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Deliver and Support (DS)



DS4.9 Offsite backup storage	• Offsite storage of all critical media, documentation and resources needed in collaboration with business process owners	• **SD 4.5.5.2 Stage 2—Requirements and strategy** • **SO 5.2.3 Backup and restore**	• *10.5.1 Information backup*
DS4.10 Post-resumption review	• Regular management assessment of plans	• *SD 4.5.5.3 Stage 3—Implementation* • *SD 4.5.5.4 Stage 4—Ongoing operation*	• *14.1.5 Testing, maintaining and reassessing business continuity plans*

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Deliver and Support (DS)

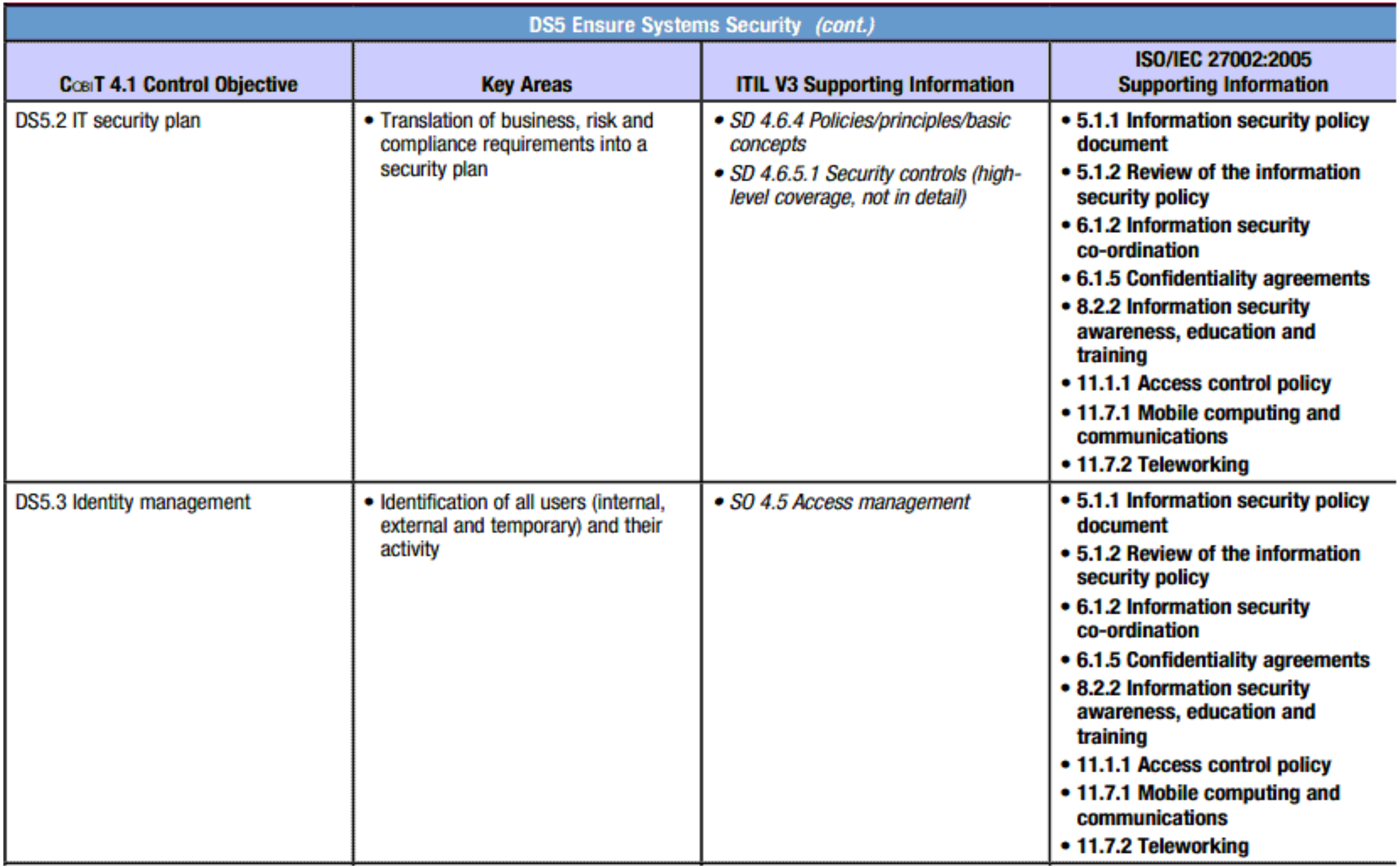


DS5 Ensure Systems Security

The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilties, policies, standards, and procedures. Security management also includes performing security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents. Effective security management protects all IT assets to minimise the business impact of security vulnerabilities and incidents.

CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS5.1 Management of IT security	• High-level placement of security management to meet business needs	• *SD 4.6 Information security management* • *SO 5.13 Information security management and service operation*	• **6.1.1 Management commitment to information security** • **6.1.2 Information security co-ordination** • **6.2.3 Addressing security in third-party agreements** • **8.2.2 Information security awareness, education and training**

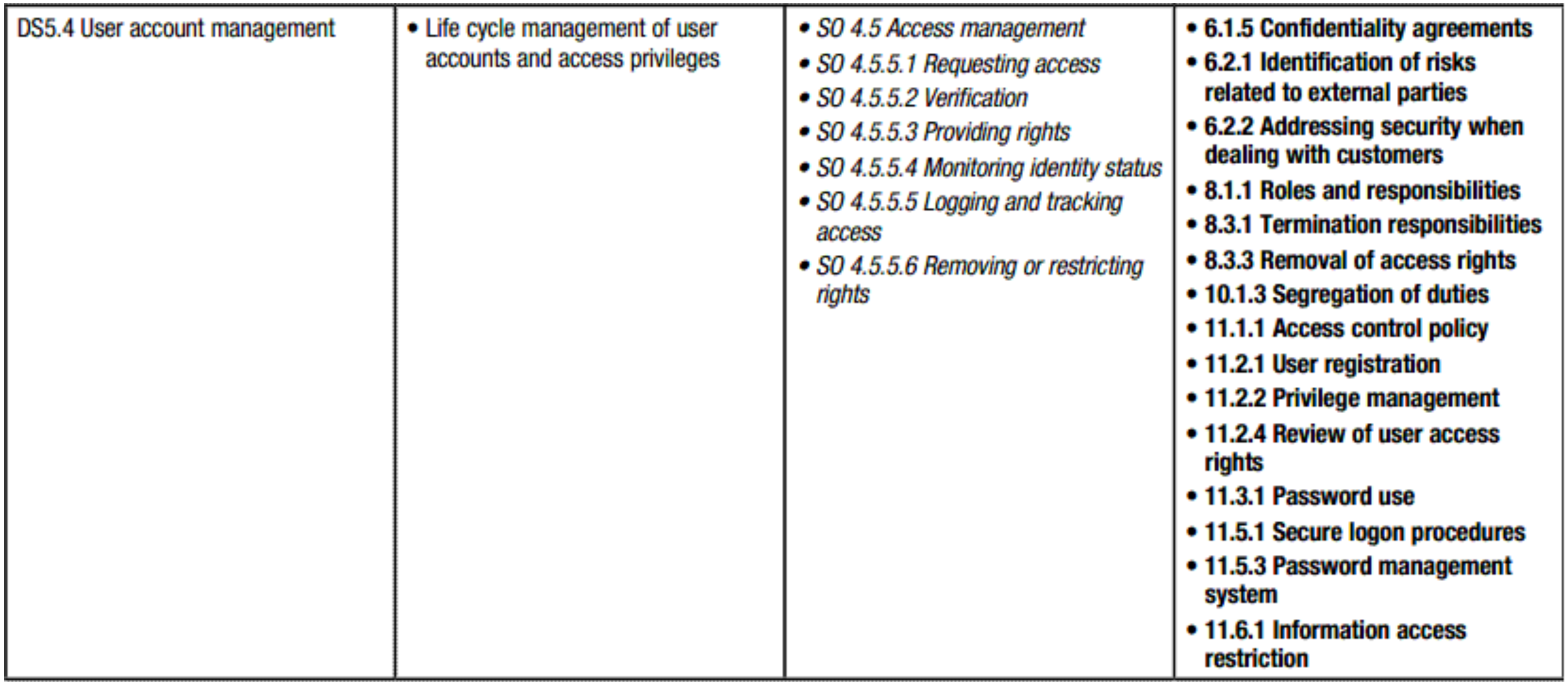
Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Deliver and Support (DS)



DS5 Ensure Systems Security *(cont.)*

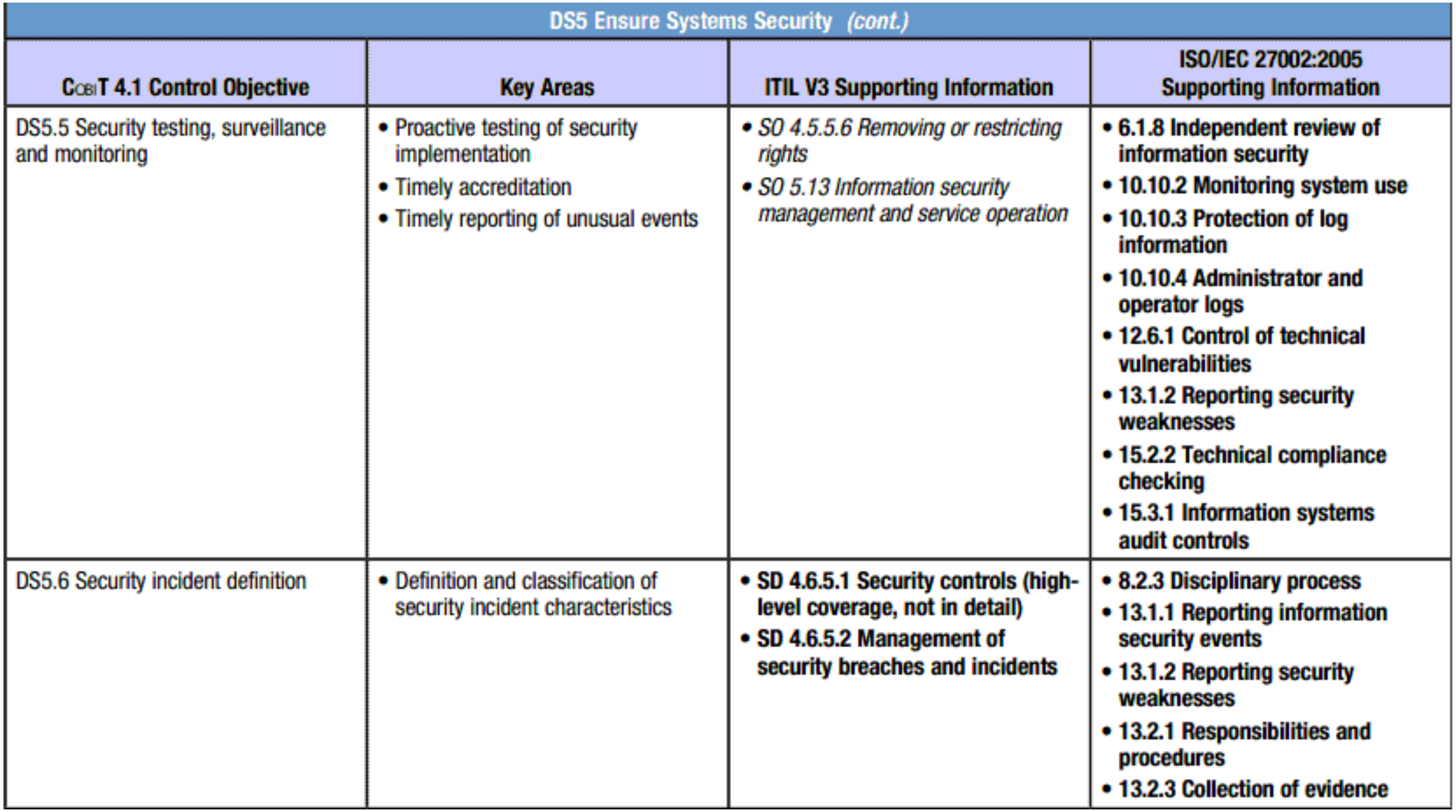
CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS5.2 IT security plan	• Translation of business, risk and compliance requirements into a security plan	• *SD 4.6.4 Policies/principles/basic concepts* • *SD 4.6.5.1 Security controls (high-level coverage, not in detail)*	• **5.1.1 Information security policy document** • **5.1.2 Review of the information security policy** • **6.1.2 Information security co-ordination** • **6.1.5 Confidentiality agreements** • **8.2.2 Information security awareness, education and training** • **11.1.1 Access control policy** • **11.7.1 Mobile computing and communications** • **11.7.2 Teleworking**
DS5.3 Identity management	• Identification of all users (internal, external and temporary) and their activity	• *SO 4.5 Access management*	• **5.1.1 Information security policy document** • **5.1.2 Review of the information security policy** • **6.1.2 Information security co-ordination** • **6.1.5 Confidentiality agreements** • **8.2.2 Information security awareness, education and training** • **11.1.1 Access control policy** • **11.7.1 Mobile computing and communications** • **11.7.2 Teleworking**

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Deliver and Support (DS)



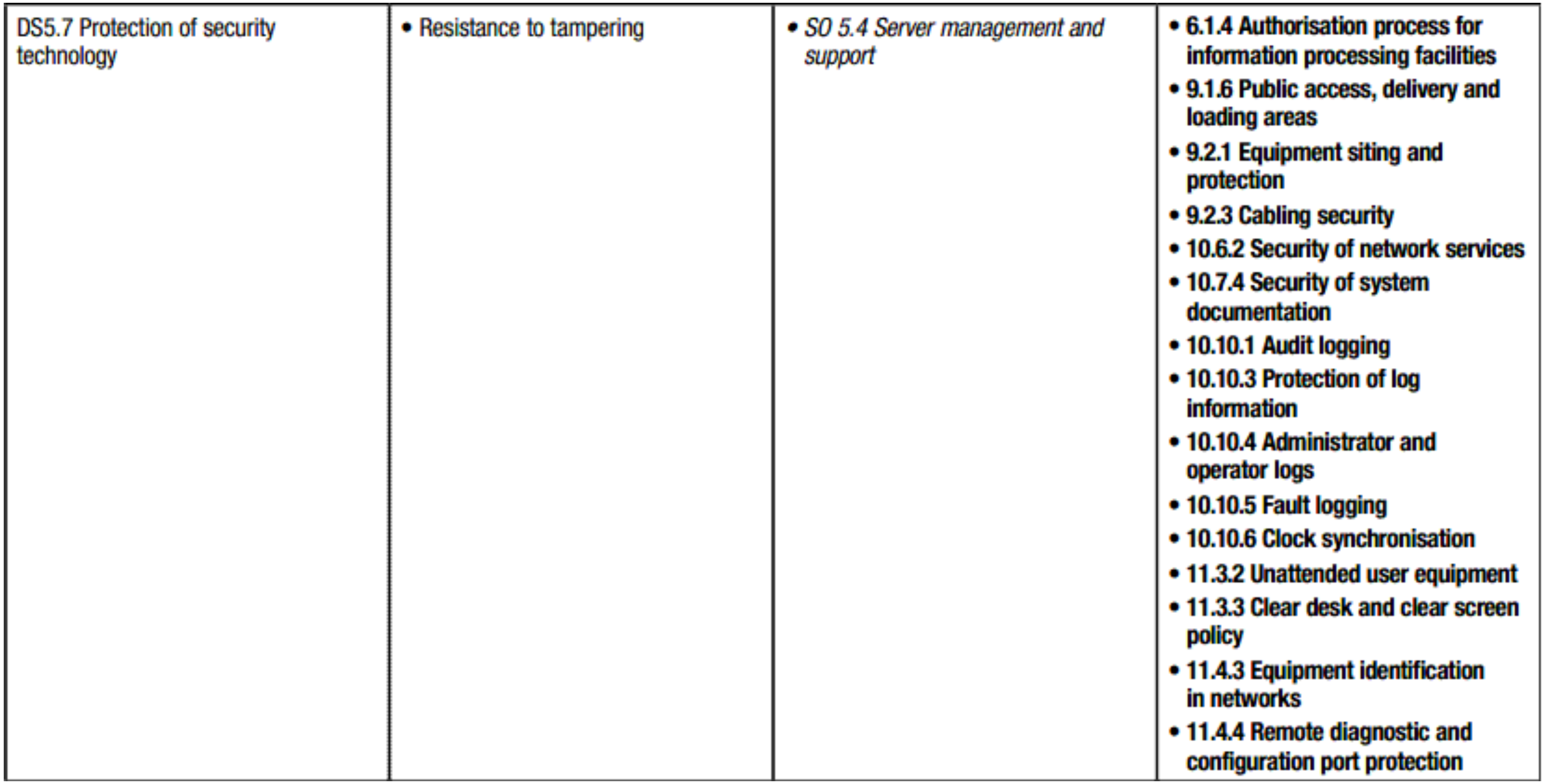
DS5.4 User account management	• Life cycle management of user accounts and access privileges	• *SO 4.5 Access management* • *SO 4.5.5.1 Requesting access* • *SO 4.5.5.2 Verification* • *SO 4.5.5.3 Providing rights* • *SO 4.5.5.4 Monitoring identity status* • *SO 4.5.5.5 Logging and tracking access* • *SO 4.5.5.6 Removing or restricting rights*	• **6.1.5 Confidentiality agreements** • **6.2.1 Identification of risks related to external parties** • **6.2.2 Addressing security when dealing with customers** • **8.1.1 Roles and responsibilities** • **8.3.1 Termination responsibilities** • **8.3.3 Removal of access rights** • **10.1.3 Segregation of duties** • **11.1.1 Access control policy** • **11.2.1 User registration** • **11.2.2 Privilege management** • **11.2.4 Review of user access rights** • **11.3.1 Password use** • **11.5.1 Secure logon procedures** • **11.5.3 Password management system** • **11.6.1 Information access restriction**

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Deliver and Support (DS)



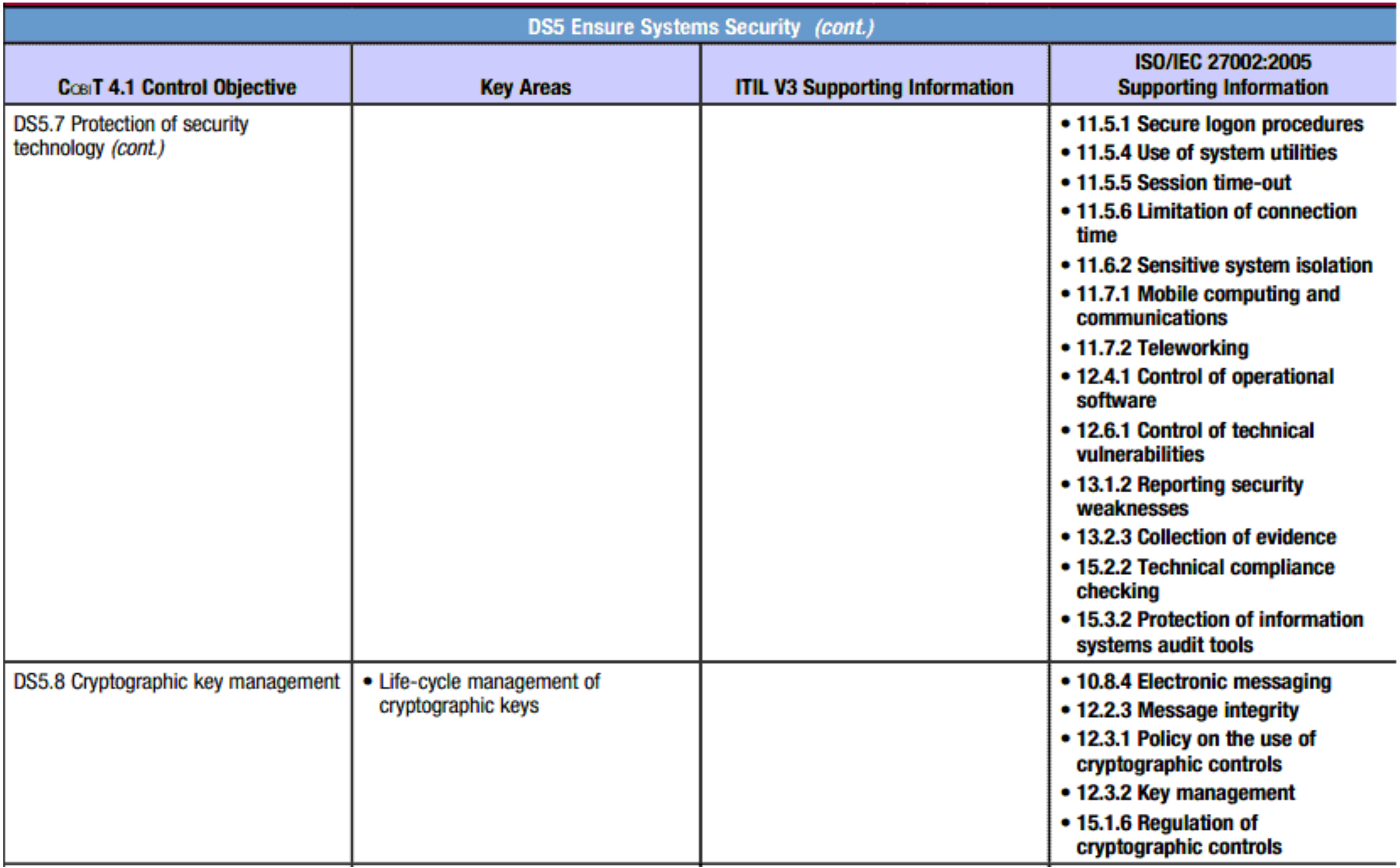
DS5 Ensure Systems Security *(cont.)*			
CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS5.5 Security testing, surveillance and monitoring	• Proactive testing of security implementation • Timely accreditation • Timely reporting of unusual events	• *SO 4.5.5.6 Removing or restricting rights* • *SO 5.13 Information security management and service operation*	• **6.1.8 Independent review of information security** • **10.10.2 Monitoring system use** • **10.10.3 Protection of log information** • **10.10.4 Administrator and operator logs** • **12.6.1 Control of technical vulnerabilities** • **13.1.2 Reporting security weaknesses** • **15.2.2 Technical compliance checking** • **15.3.1 Information systems audit controls**
DS5.6 Security incident definition	• Definition and classification of security incident characteristics	• **SD 4.6.5.1 Security controls (high-level coverage, not in detail)** • **SD 4.6.5.2 Management of security breaches and incidents**	• **8.2.3 Disciplinary process** • **13.1.1 Reporting information security events** • **13.1.2 Reporting security weaknesses** • **13.2.1 Responsibilities and procedures** • **13.2.3 Collection of evidence**

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Deliver and Support (DS)



DS5.7 Protection of security technology	• Resistance to tampering	• *SO 5.4 Server management and support*	• **6.1.4 Authorisation process for information processing facilities** • **9.1.6 Public access, delivery and loading areas** • **9.2.1 Equipment siting and protection** • **9.2.3 Cabling security** • **10.6.2 Security of network services** • **10.7.4 Security of system documentation** • **10.10.1 Audit logging** • **10.10.3 Protection of log information** • **10.10.4 Administrator and operator logs** • **10.10.5 Fault logging** • **10.10.6 Clock synchronisation** • **11.3.2 Unattended user equipment** • **11.3.3 Clear desk and clear screen policy** • **11.4.3 Equipment identification in networks** • **11.4.4 Remote diagnostic and configuration port protection**

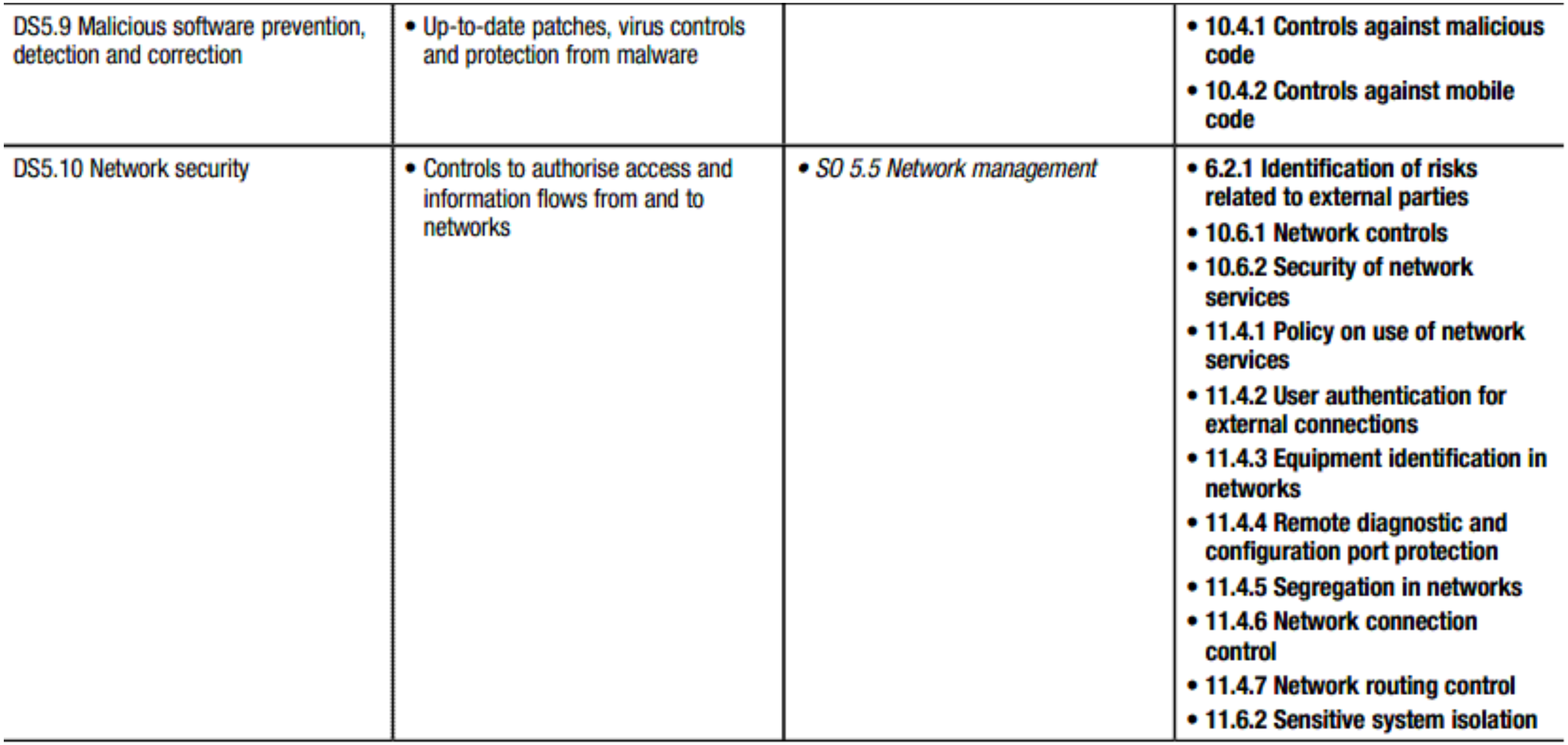
Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Deliver and Support (DS)



DS5 Ensure Systems Security *(cont.)*

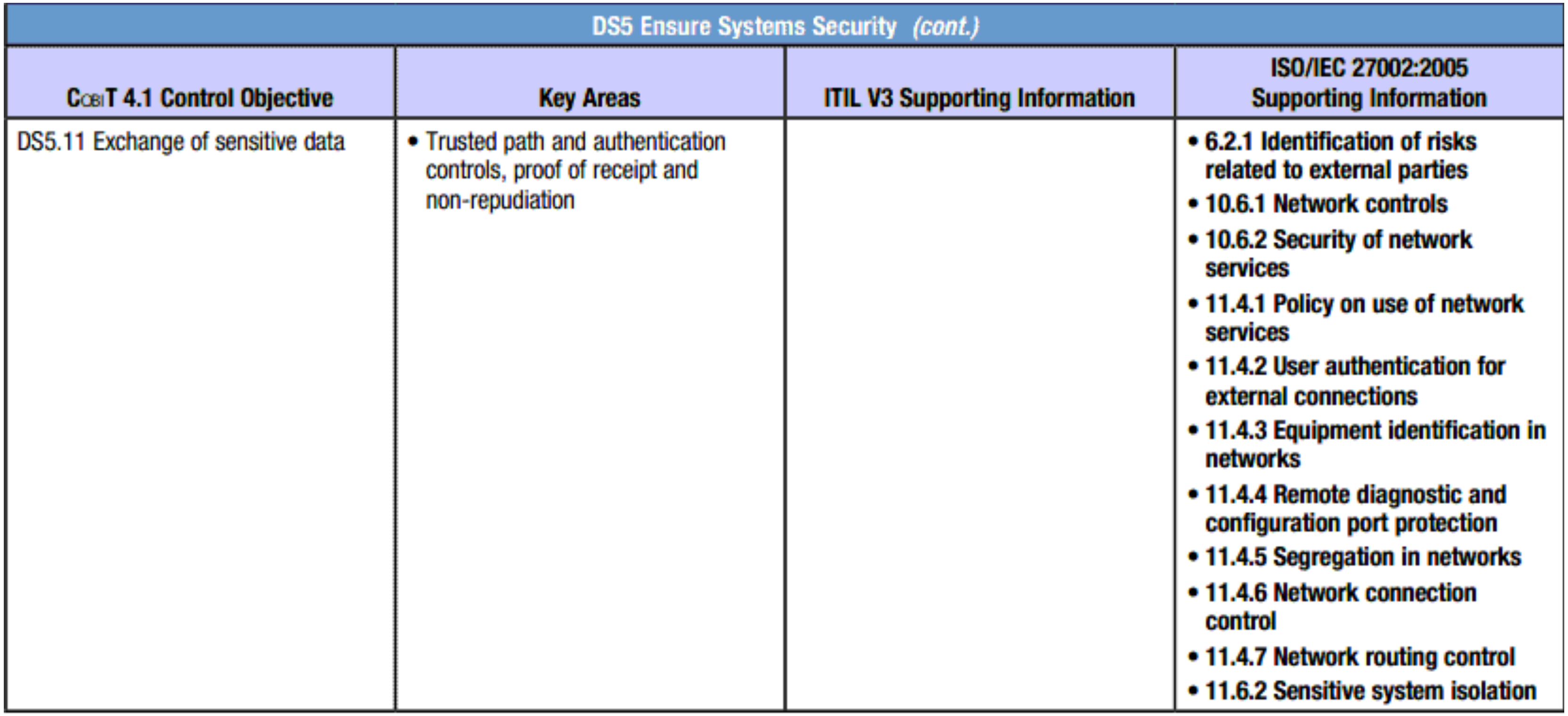
CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS5.7 Protection of security technology *(cont.)*			• 11.5.1 Secure logon procedures • 11.5.4 Use of system utilities • 11.5.5 Session time-out • 11.5.6 Limitation of connection time • 11.6.2 Sensitive system isolation • 11.7.1 Mobile computing and communications • 11.7.2 Teleworking • 12.4.1 Control of operational software • 12.6.1 Control of technical vulnerabilities • 13.1.2 Reporting security weaknesses • 13.2.3 Collection of evidence • 15.2.2 Technical compliance checking • 15.3.2 Protection of information systems audit tools
DS5.8 Cryptographic key management	• Life-cycle management of cryptographic keys		• 10.8.4 Electronic messaging • 12.2.3 Message integrity • 12.3.1 Policy on the use of cryptographic controls • 12.3.2 Key management • 15.1.6 Regulation of cryptographic controls

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Deliver and Support (DS)



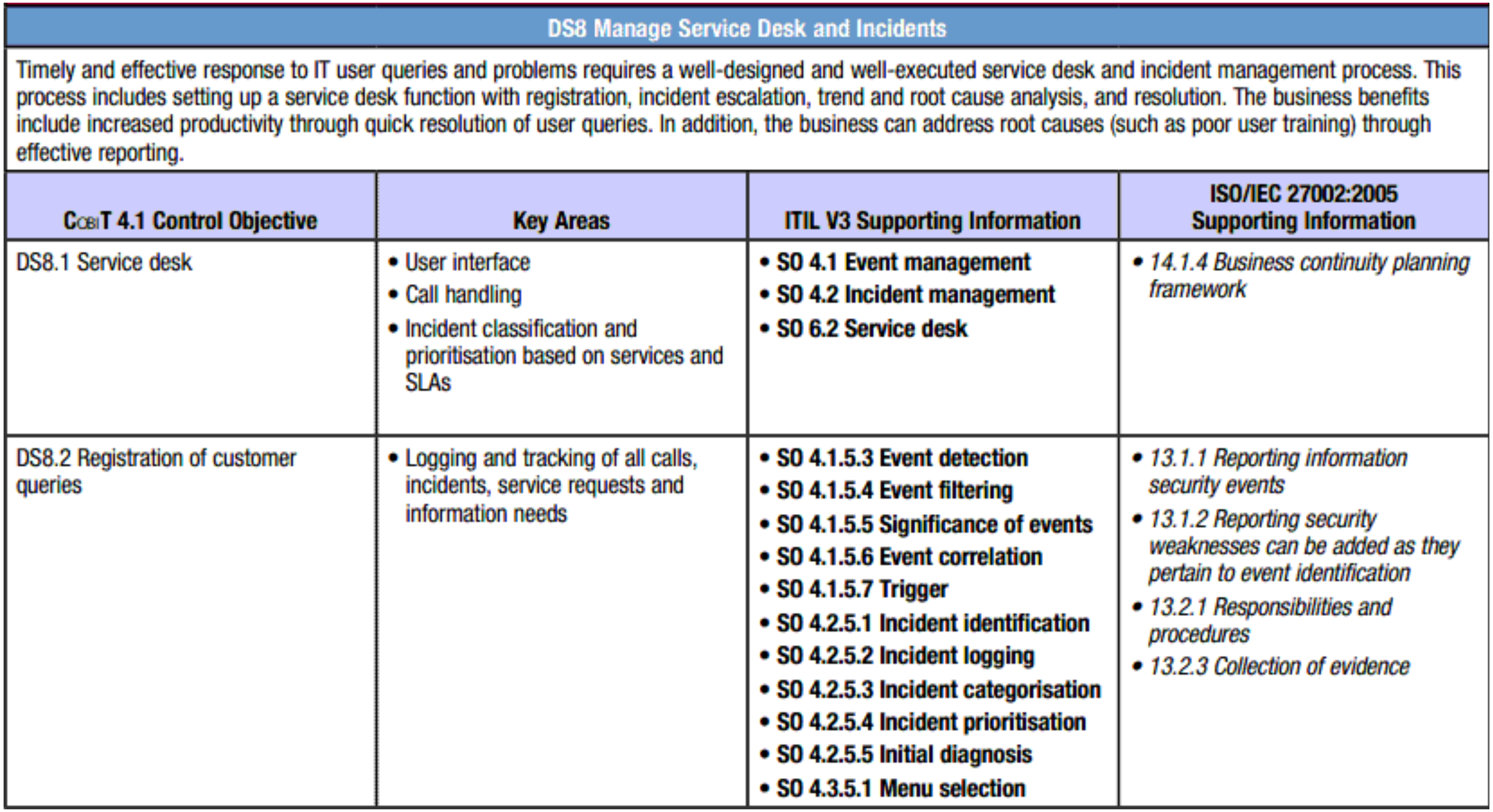
DS5.9 Malicious software prevention, detection and correction	• Up-to-date patches, virus controls and protection from malware		• **10.4.1 Controls against malicious code** • **10.4.2 Controls against mobile code**
DS5.10 Network security	• Controls to authorise access and information flows from and to networks	• *SO 5.5 Network management*	• **6.2.1 Identification of risks related to external parties** • **10.6.1 Network controls** • **10.6.2 Security of network services** • **11.4.1 Policy on use of network services** • **11.4.2 User authentication for external connections** • **11.4.3 Equipment identification in networks** • **11.4.4 Remote diagnostic and configuration port protection** • **11.4.5 Segregation in networks** • **11.4.6 Network connection control** • **11.4.7 Network routing control** • **11.6.2 Sensitive system isolation**

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Deliver and Support (DS)



DS5 Ensure Systems Security *(cont.)*			
CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS5.11 Exchange of sensitive data	• Trusted path and authentication controls, proof of receipt and non-repudiation		• 6.2.1 Identification of risks related to external parties • 10.6.1 Network controls • 10.6.2 Security of network services • 11.4.1 Policy on use of network services • 11.4.2 User authentication for external connections • 11.4.3 Equipment identification in networks • 11.4.4 Remote diagnostic and configuration port protection • 11.4.5 Segregation in networks • 11.4.6 Network connection control • 11.4.7 Network routing control • 11.6.2 Sensitive system isolation

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Deliver and Support (DS)

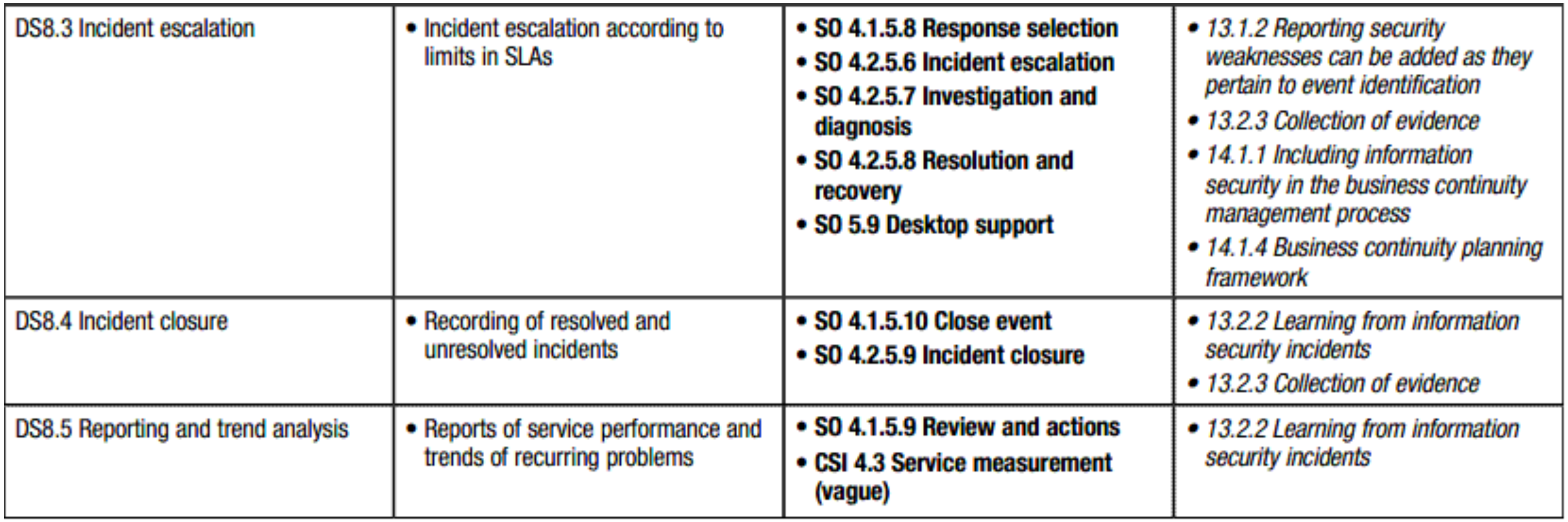


DS8 Manage Service Desk and Incidents

Timely and effective response to IT user queries and problems requires a well-designed and well-executed service desk and incident management process. This process includes setting up a service desk function with registration, incident escalation, trend and root cause analysis, and resolution. The business benefits include increased productivity through quick resolution of user queries. In addition, the business can address root causes (such as poor user training) through effective reporting.

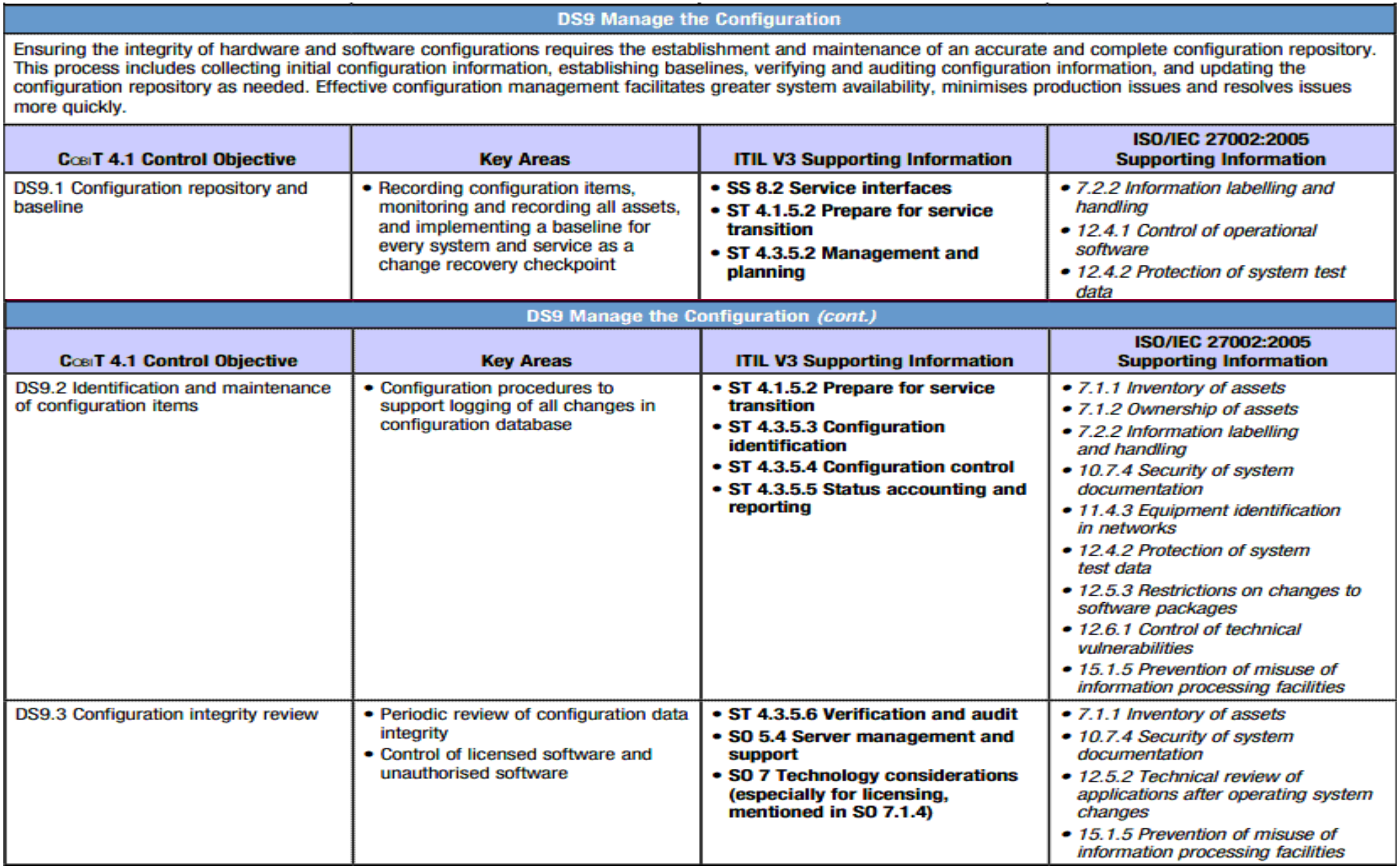
CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS8.1 Service desk	• User interface • Call handling • Incident classification and prioritisation based on services and SLAs	• **SO 4.1 Event management** • **SO 4.2 Incident management** • **SO 6.2 Service desk**	• *14.1.4 Business continuity planning framework*
DS8.2 Registration of customer queries	• Logging and tracking of all calls, incidents, service requests and information needs	• **SO 4.1.5.3 Event detection** • **SO 4.1.5.4 Event filtering** • **SO 4.1.5.5 Significance of events** • **SO 4.1.5.6 Event correlation** • **SO 4.1.5.7 Trigger** • **SO 4.2.5.1 Incident identification** • **SO 4.2.5.2 Incident logging** • **SO 4.2.5.3 Incident categorisation** • **SO 4.2.5.4 Incident prioritisation** • **SO 4.2.5.5 Initial diagnosis** • **SO 4.3.5.1 Menu selection**	• *13.1.1 Reporting information security events* • *13.1.2 Reporting security weaknesses can be added as they pertain to event identification* • *13.2.1 Responsibilities and procedures* • *13.2.3 Collection of evidence*

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Deliver and Support (DS)



DS8.3 Incident escalation	• Incident escalation according to limits in SLAs	• **SO 4.1.5.8 Response selection** • **SO 4.2.5.6 Incident escalation** • **SO 4.2.5.7 Investigation and diagnosis** • **SO 4.2.5.8 Resolution and recovery** • **SO 5.9 Desktop support**	• *13.1.2 Reporting security weaknesses can be added as they pertain to event identification* • *13.2.3 Collection of evidence* • *14.1.1 Including information security in the business continuity management process* • *14.1.4 Business continuity planning framework*
DS8.4 Incident closure	• Recording of resolved and unresolved incidents	• **SO 4.1.5.10 Close event** • **SO 4.2.5.9 Incident closure**	• *13.2.2 Learning from information security incidents* • *13.2.3 Collection of evidence*
DS8.5 Reporting and trend analysis	• Reports of service performance and trends of recurring problems	• **SO 4.1.5.9 Review and actions** • **CSI 4.3 Service measurement (vague)**	• *13.2.2 Learning from information security incidents*

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Deliver and Support (DS)



DS9 Manage the Configuration

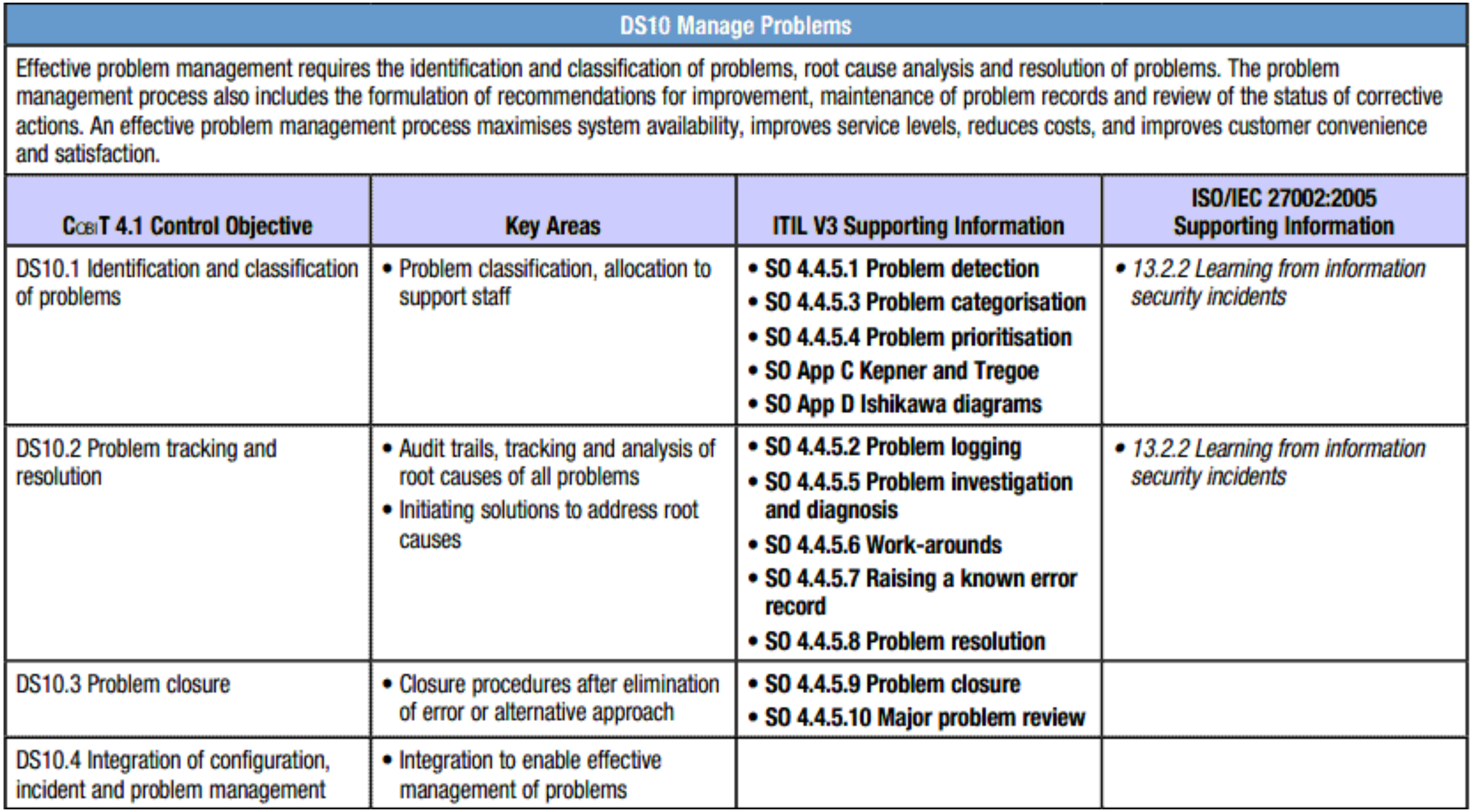
Ensuring the integrity of hardware and software configurations requires the establishment and maintenance of an accurate and complete configuration repository. This process includes collecting initial configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository as needed. Effective configuration management facilitates greater system availability, minimises production issues and resolves issues more quickly.

CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS9.1 Configuration repository and baseline	• Recording configuration items, monitoring and recording all assets, and implementing a baseline for every system and service as a change recovery checkpoint	• **SS 8.2 Service interfaces** • **ST 4.1.5.2 Prepare for service transition** • **ST 4.3.5.2 Management and planning**	• *7.2.2 Information labelling and handling* • *12.4.1 Control of operational software* • *12.4.2 Protection of system test data*

DS9 Manage the Configuration *(cont.)*

CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS9.2 Identification and maintenance of configuration items	• Configuration procedures to support logging of all changes in configuration database	• **ST 4.1.5.2 Prepare for service transition** • **ST 4.3.5.3 Configuration identification** • **ST 4.3.5.4 Configuration control** • **ST 4.3.5.5 Status accounting and reporting**	• *7.1.1 Inventory of assets* • *7.1.2 Ownership of assets* • *7.2.2 Information labelling and handling* • *10.7.4 Security of system documentation* • *11.4.3 Equipment identification in networks* • *12.4.2 Protection of system test data* • *12.5.3 Restrictions on changes to software packages* • *12.6.1 Control of technical vulnerabilities* • *15.1.5 Prevention of misuse of information processing facilities*
DS9.3 Configuration integrity review	• Periodic review of configuration data integrity • Control of licensed software and unauthorised software	• **ST 4.3.5.6 Verification and audit** • **SO 5.4 Server management and support** • **SO 7 Technology considerations (especially for licensing, mentioned in SO 7.1.4)**	• *7.1.1 Inventory of assets* • *10.7.4 Security of system documentation* • *12.5.2 Technical review of applications after operating system changes* • *15.1.5 Prevention of misuse of information processing facilities*

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Deliver and Support (DS)

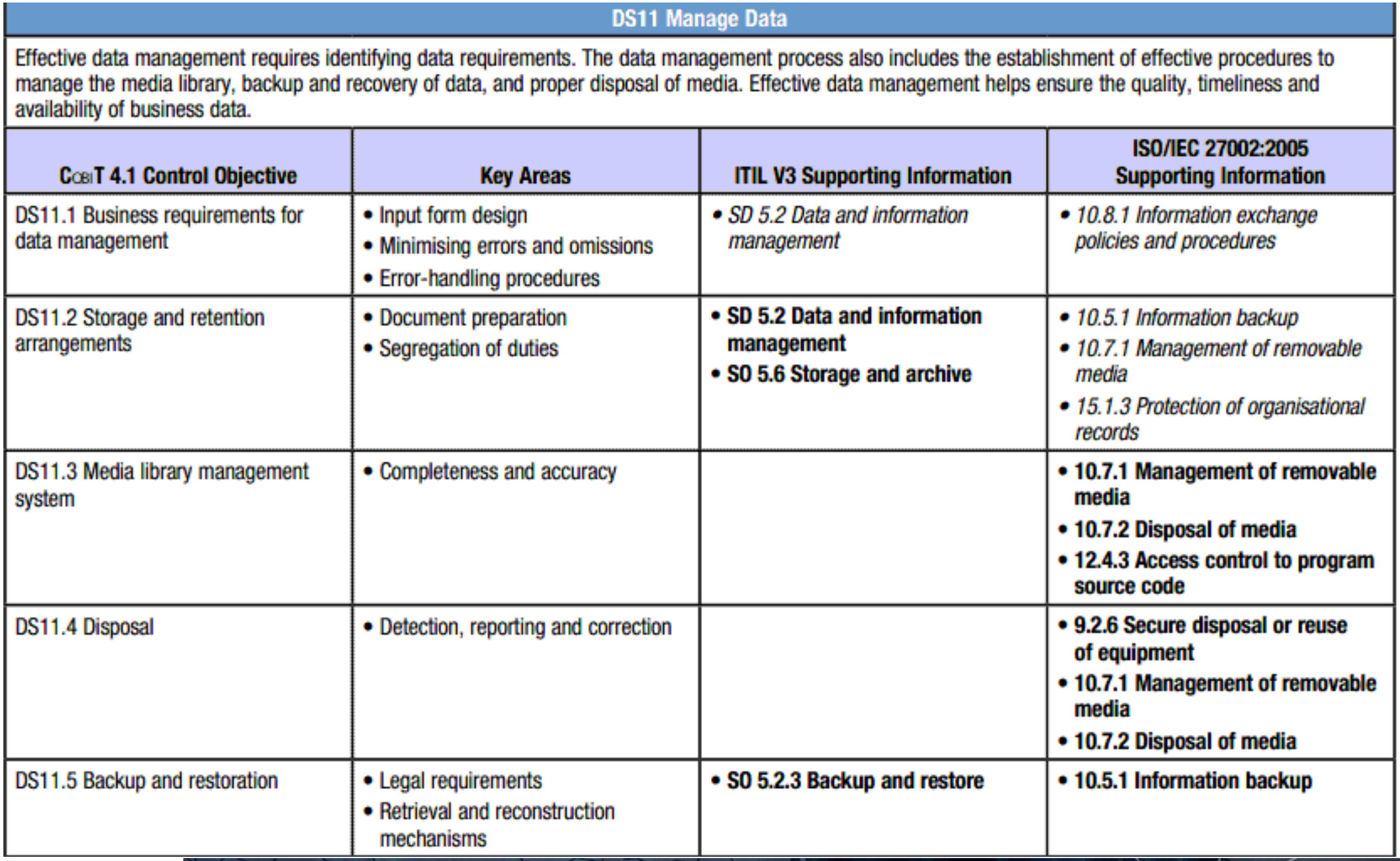


DS10 Manage Problems

Effective problem management requires the identification and classification of problems, root cause analysis and resolution of problems. The problem management process also includes the formulation of recommendations for improvement, maintenance of problem records and review of the status of corrective actions. An effective problem management process maximises system availability, improves service levels, reduces costs, and improves customer convenience and satisfaction.

CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS10.1 Identification and classification of problems	• Problem classification, allocation to support staff	• **SO 4.4.5.1 Problem detection** • **SO 4.4.5.3 Problem categorisation** • **SO 4.4.5.4 Problem prioritisation** • **SO App C Kepner and Tregoe** • **SO App D Ishikawa diagrams**	• *13.2.2 Learning from information security incidents*
DS10.2 Problem tracking and resolution	• Audit trails, tracking and analysis of root causes of all problems • Initiating solutions to address root causes	• **SO 4.4.5.2 Problem logging** • **SO 4.4.5.5 Problem investigation and diagnosis** • **SO 4.4.5.6 Work-arounds** • **SO 4.4.5.7 Raising a known error record** • **SO 4.4.5.8 Problem resolution**	• *13.2.2 Learning from information security incidents*
DS10.3 Problem closure	• Closure procedures after elimination of error or alternative approach	• **SO 4.4.5.9 Problem closure** • **SO 4.4.5.10 Major problem review**	
DS10.4 Integration of configuration, incident and problem management	• Integration to enable effective management of problems		

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Deliver and Support (DS)

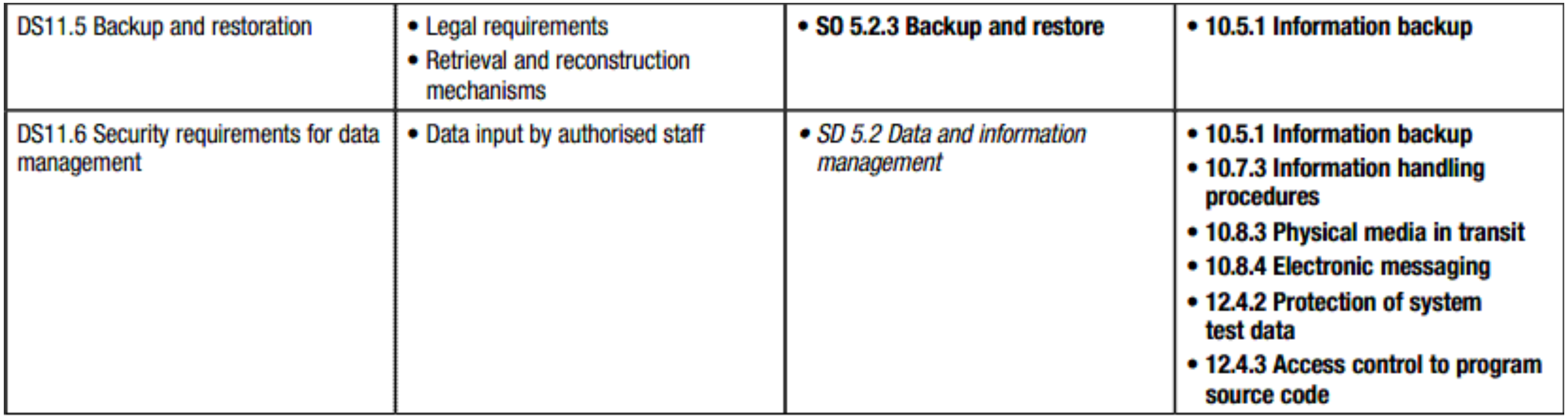


DS11 Manage Data

Effective data management requires identifying data requirements. The data management process also includes the establishment of effective procedures to manage the media library, backup and recovery of data, and proper disposal of media. Effective data management helps ensure the quality, timeliness and availability of business data.

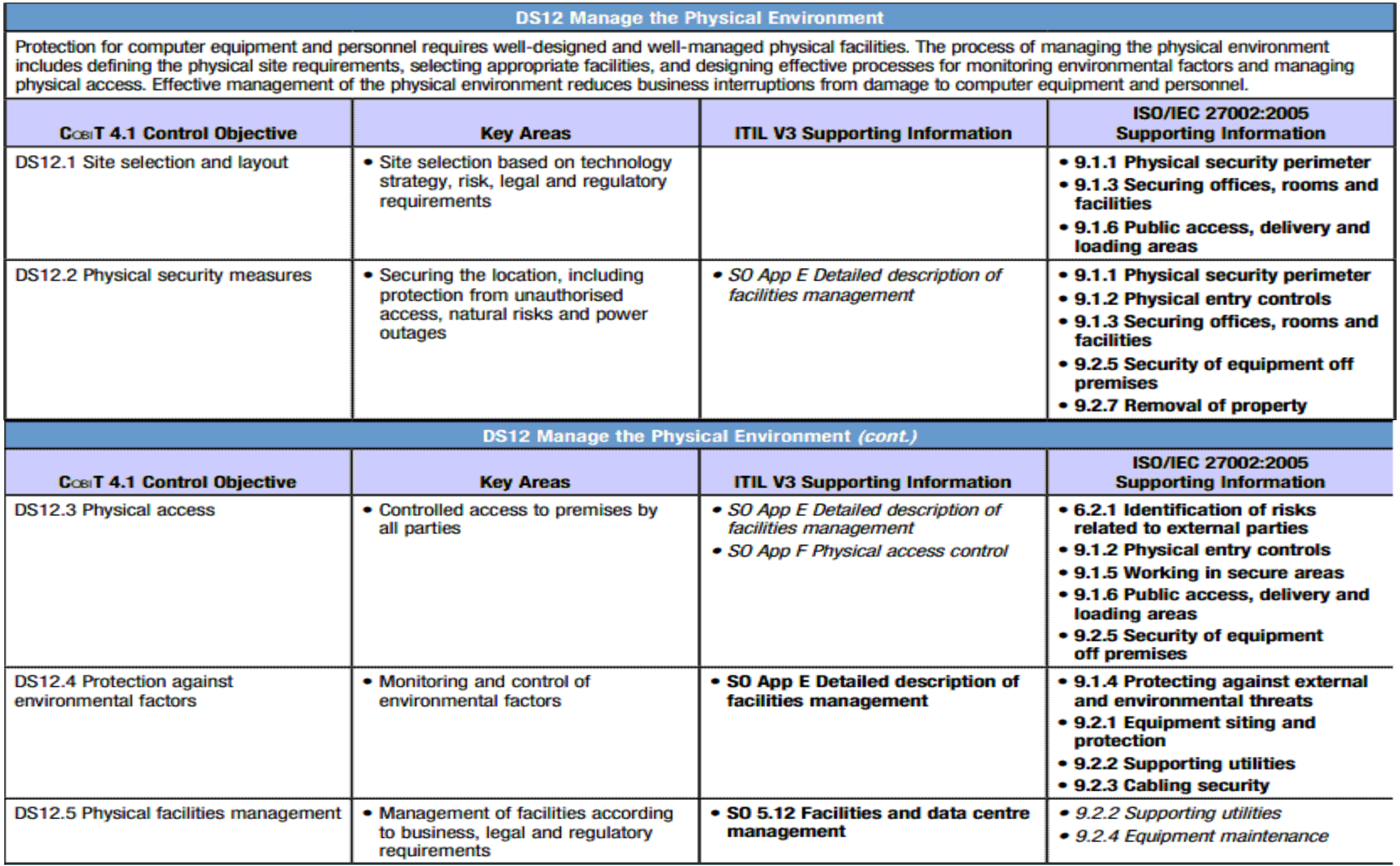
CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS11.1 Business requirements for data management	• Input form design • Minimising errors and omissions • Error-handling procedures	• *SD 5.2 Data and information management*	• *10.8.1 Information exchange policies and procedures*
DS11.2 Storage and retention arrangements	• Document preparation • Segregation of duties	• **SD 5.2 Data and information management** • **SO 5.6 Storage and archive**	• *10.5.1 Information backup* • *10.7.1 Management of removable media* • *15.1.3 Protection of organisational records*
DS11.3 Media library management system	• Completeness and accuracy		• **10.7.1 Management of removable media** • **10.7.2 Disposal of media** • **12.4.3 Access control to program source code**
DS11.4 Disposal	• Detection, reporting and correction		• **9.2.6 Secure disposal or reuse of equipment** • **10.7.1 Management of removable media** • **10.7.2 Disposal of media**
DS11.5 Backup and restoration	• Legal requirements • Retrieval and reconstruction mechanisms	• **SO 5.2.3 Backup and restore**	• **10.5.1 Information backup**

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Deliver and Support (DS)



DS11.5 Backup and restoration	• Legal requirements • Retrieval and reconstruction mechanisms	• **SO 5.2.3 Backup and restore**	• **10.5.1 Information backup**
DS11.6 Security requirements for data management	• Data input by authorised staff	• *SD 5.2 Data and information management*	• **10.5.1 Information backup** • **10.7.3 Information handling procedures** • **10.8.3 Physical media in transit** • **10.8.4 Electronic messaging** • **12.4.2 Protection of system test data** • **12.4.3 Access control to program source code**

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Deliver and Support (DS)



DS12 Manage the Physical Environment

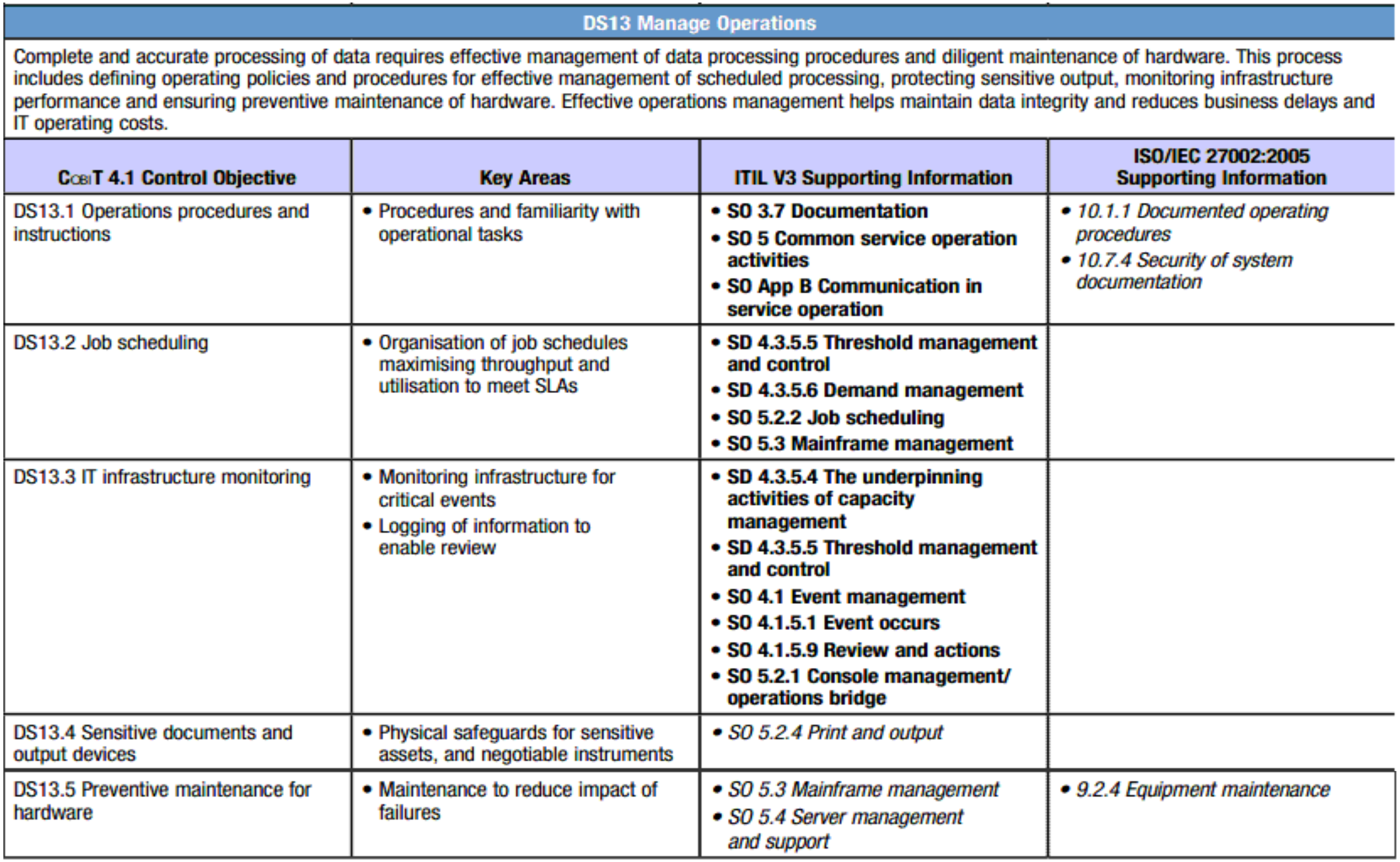
Protection for computer equipment and personnel requires well-designed and well-managed physical facilities. The process of managing the physical environment includes defining the physical site requirements, selecting appropriate facilities, and designing effective processes for monitoring environmental factors and managing physical access. Effective management of the physical environment reduces business interruptions from damage to computer equipment and personnel.

CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS12.1 Site selection and layout	• Site selection based on technology strategy, risk, legal and regulatory requirements		• **9.1.1 Physical security perimeter** • **9.1.3 Securing offices, rooms and facilities** • **9.1.6 Public access, delivery and loading areas**
DS12.2 Physical security measures	• Securing the location, including protection from unauthorised access, natural risks and power outages	• *SO App E Detailed description of facilities management*	• **9.1.1 Physical security perimeter** • **9.1.2 Physical entry controls** • **9.1.3 Securing offices, rooms and facilities** • **9.2.5 Security of equipment off premises** • **9.2.7 Removal of property**

DS12 Manage the Physical Environment *(cont.)*

CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS12.3 Physical access	• Controlled access to premises by all parties	• *SO App E Detailed description of facilities management* • *SO App F Physical access control*	• **6.2.1 Identification of risks related to external parties** • **9.1.2 Physical entry controls** • **9.1.5 Working in secure areas** • **9.1.6 Public access, delivery and loading areas** • **9.2.5 Security of equipment off premises**
DS12.4 Protection against environmental factors	• Monitoring and control of environmental factors	• **SO App E Detailed description of facilities management**	• **9.1.4 Protecting against external and environmental threats** • **9.2.1 Equipment siting and protection** • **9.2.2 Supporting utilities** • **9.2.3 Cabling security**
DS12.5 Physical facilities management	• Management of facilities according to business, legal and regulatory requirements	• **SO 5.12 Facilities and data centre management**	• *9.2.2 Supporting utilities* • *9.2.4 Equipment maintenance*

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Deliver and Support (DS)

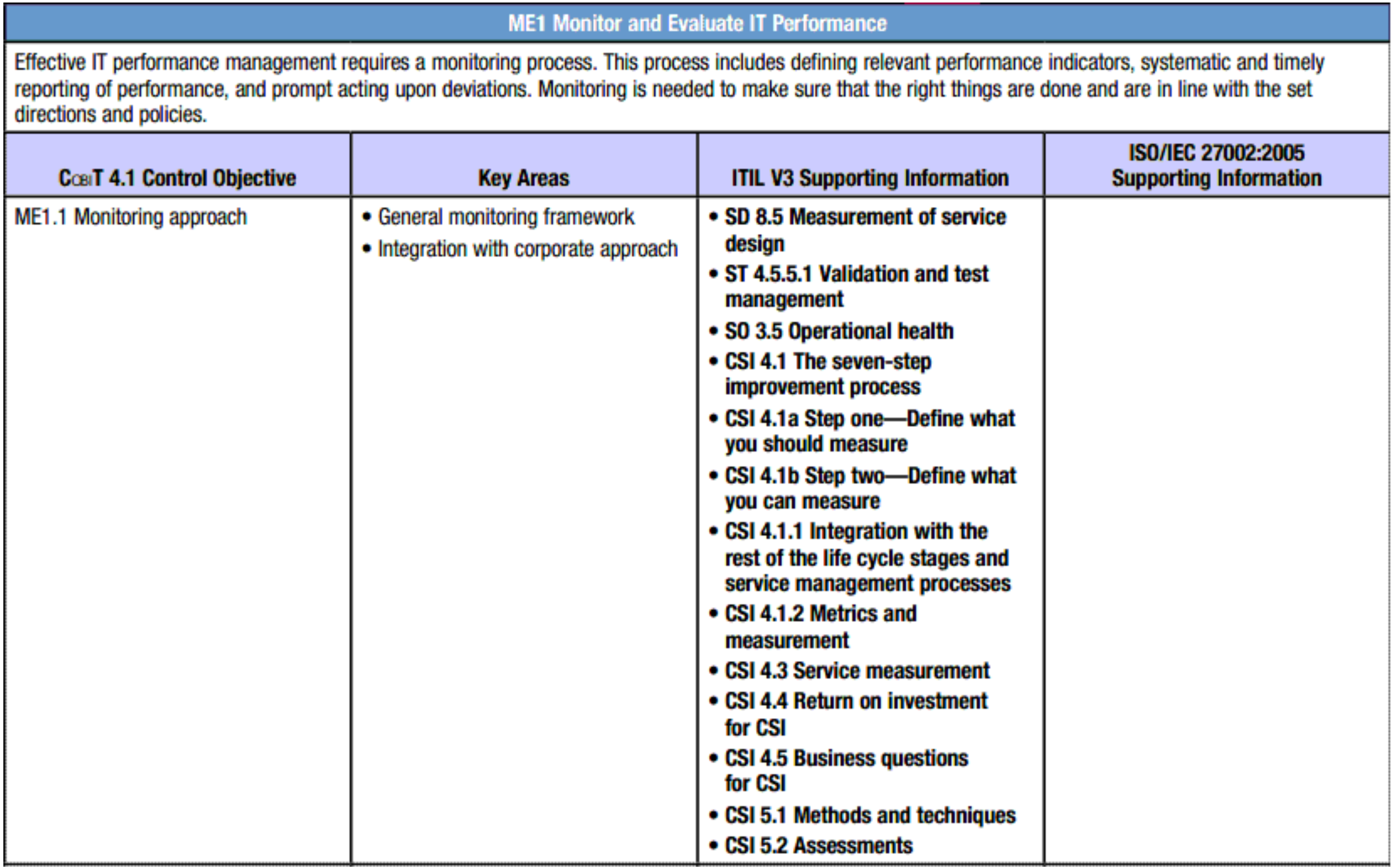


DS13 Manage Operations

Complete and accurate processing of data requires effective management of data processing procedures and diligent maintenance of hardware. This process includes defining operating policies and procedures for effective management of scheduled processing, protecting sensitive output, monitoring infrastructure performance and ensuring preventive maintenance of hardware. Effective operations management helps maintain data integrity and reduces business delays and IT operating costs.

CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS13.1 Operations procedures and instructions	• Procedures and familiarity with operational tasks	• **SO 3.7 Documentation** • **SO 5 Common service operation activities** • **SO App B Communication in service operation**	• *10.1.1 Documented operating procedures* • *10.7.4 Security of system documentation*
DS13.2 Job scheduling	• Organisation of job schedules maximising throughput and utilisation to meet SLAs	• **SD 4.3.5.5 Threshold management and control** • **SD 4.3.5.6 Demand management** • **SO 5.2.2 Job scheduling** • **SO 5.3 Mainframe management**	
DS13.3 IT infrastructure monitoring	• Monitoring infrastructure for critical events • Logging of information to enable review	• **SD 4.3.5.4 The underpinning activities of capacity management** • **SD 4.3.5.5 Threshold management and control** • **SO 4.1 Event management** • **SO 4.1.5.1 Event occurs** • **SO 4.1.5.9 Review and actions** • **SO 5.2.1 Console management/ operations bridge**	
DS13.4 Sensitive documents and output devices	• Physical safeguards for sensitive assets, and negotiable instruments	• *SO 5.2.4 Print and output*	
DS13.5 Preventive maintenance for hardware	• Maintenance to reduce impact of failures	• *SO 5.3 Mainframe management* • *SO 5.4 Server management and support*	• *9.2.4 Equipment maintenance*

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Monitor and Evaluate (ME)

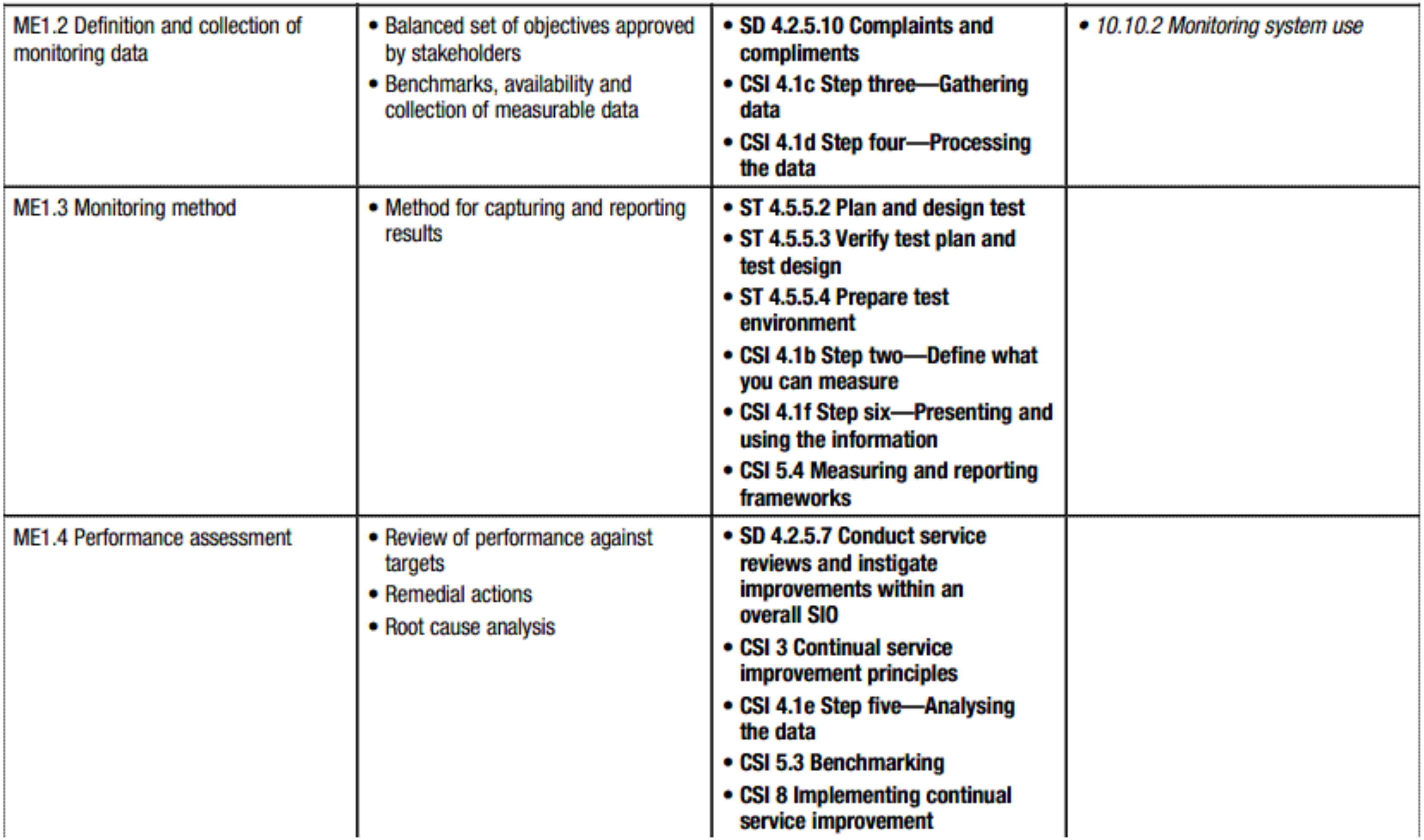


ME1 Monitor and Evaluate IT Performance

Effective IT performance management requires a monitoring process. This process includes defining relevant performance indicators, systematic and timely reporting of performance, and prompt acting upon deviations. Monitoring is needed to make sure that the right things are done and are in line with the set directions and policies.

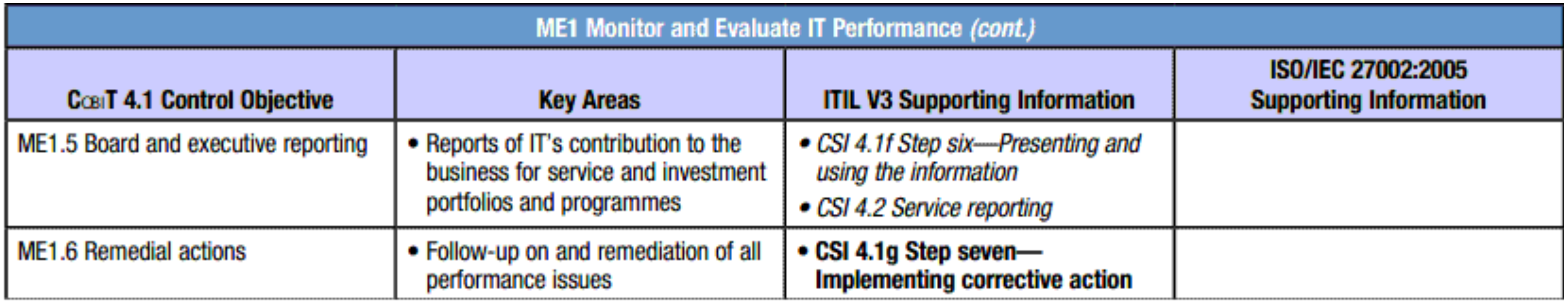
CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
ME1.1 Monitoring approach	• General monitoring framework • Integration with corporate approach	• SD 8.5 Measurement of service design • ST 4.5.5.1 Validation and test management • SO 3.5 Operational health • CSI 4.1 The seven-step improvement process • CSI 4.1a Step one—Define what you should measure • CSI 4.1b Step two—Define what you can measure • CSI 4.1.1 Integration with the rest of the life cycle stages and service management processes • CSI 4.1.2 Metrics and measurement • CSI 4.3 Service measurement • CSI 4.4 Return on investment for CSI • CSI 4.5 Business questions for CSI • CSI 5.1 Methods and techniques • CSI 5.2 Assessments	

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Monitor and Evaluate (ME)



ME1.2 Definition and collection of monitoring data	• Balanced set of objectives approved by stakeholders • Benchmarks, availability and collection of measurable data	• **SD 4.2.5.10 Complaints and compliments** • **CSI 4.1c Step three—Gathering data** • **CSI 4.1d Step four—Processing the data**	• *10.10.2 Monitoring system use*
ME1.3 Monitoring method	• Method for capturing and reporting results	• **ST 4.5.5.2 Plan and design test** • **ST 4.5.5.3 Verify test plan and test design** • **ST 4.5.5.4 Prepare test environment** • **CSI 4.1b Step two—Define what you can measure** • **CSI 4.1f Step six—Presenting and using the information** • **CSI 5.4 Measuring and reporting frameworks**	
ME1.4 Performance assessment	• Review of performance against targets • Remedial actions • Root cause analysis	• **SD 4.2.5.7 Conduct service reviews and instigate improvements within an overall SIO** • **CSI 3 Continual service improvement principles** • **CSI 4.1e Step five—Analysing the data** • **CSI 5.3 Benchmarking** • **CSI 8 Implementing continual service improvement**	

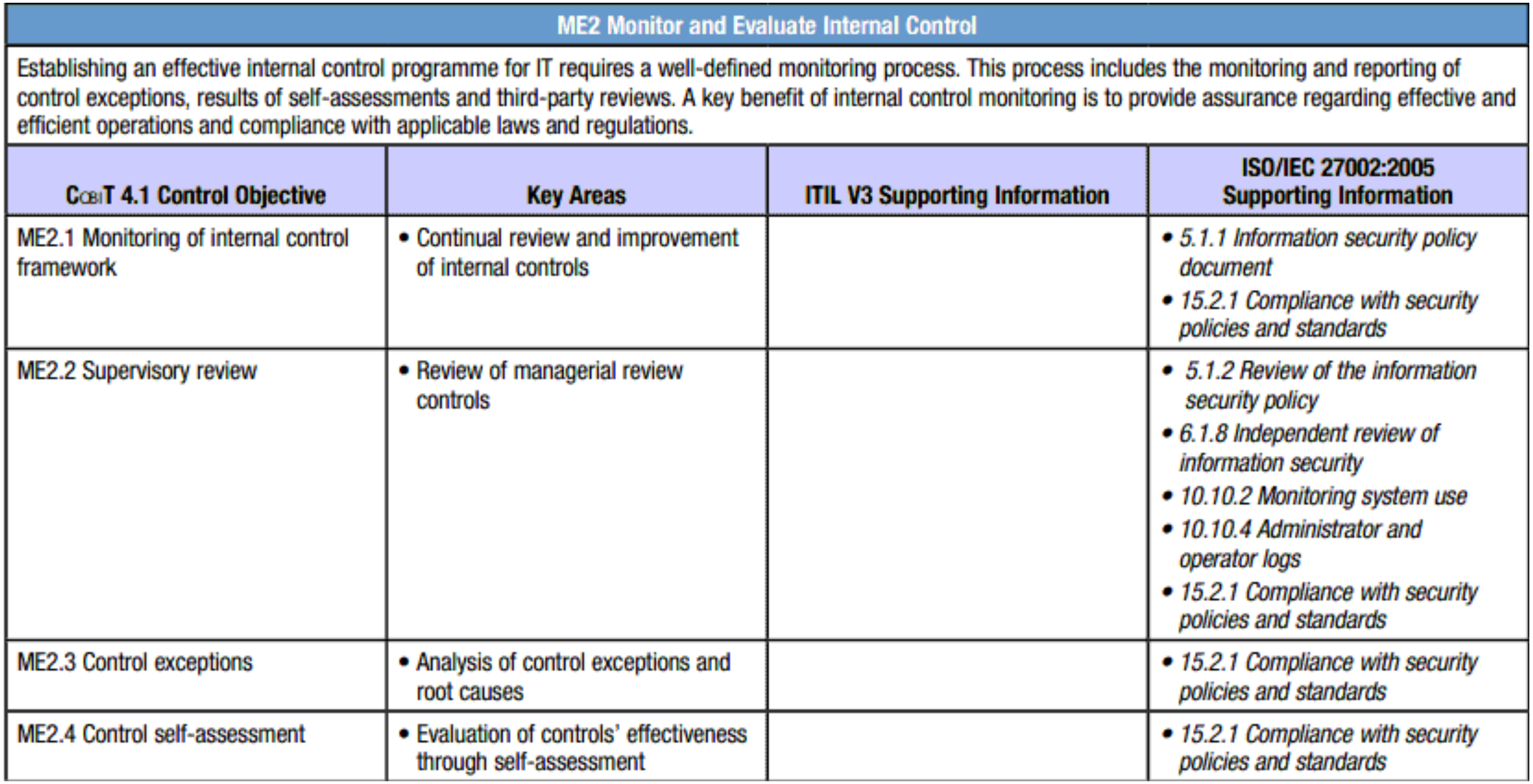
Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Monitor and Evaluate (ME)



ME1 Monitor and Evaluate IT Performance *(cont.)*

CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
ME1.5 Board and executive reporting	• Reports of IT's contribution to the business for service and investment portfolios and programmes	• *CSI 4.1f Step six—Presenting and using the information* • *CSI 4.2 Service reporting*	
ME1.6 Remedial actions	• Follow-up on and remediation of all performance issues	• **CSI 4.1g Step seven—Implementing corrective action**	

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Monitor and Evaluate (ME)

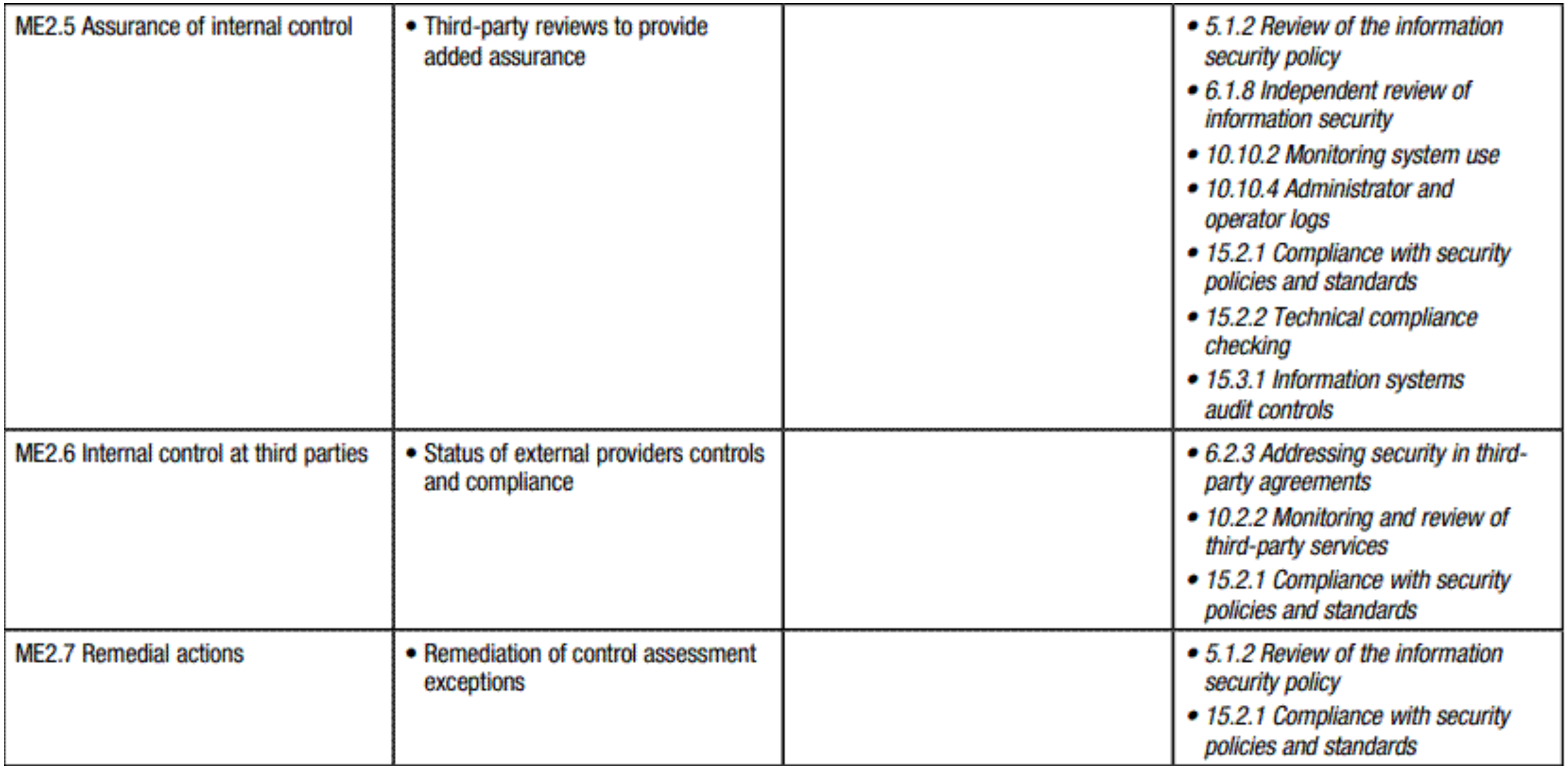


ME2 Monitor and Evaluate Internal Control

Establishing an effective internal control programme for IT requires a well-defined monitoring process. This process includes the monitoring and reporting of control exceptions, results of self-assessments and third-party reviews. A key benefit of internal control monitoring is to provide assurance regarding effective and efficient operations and compliance with applicable laws and regulations.

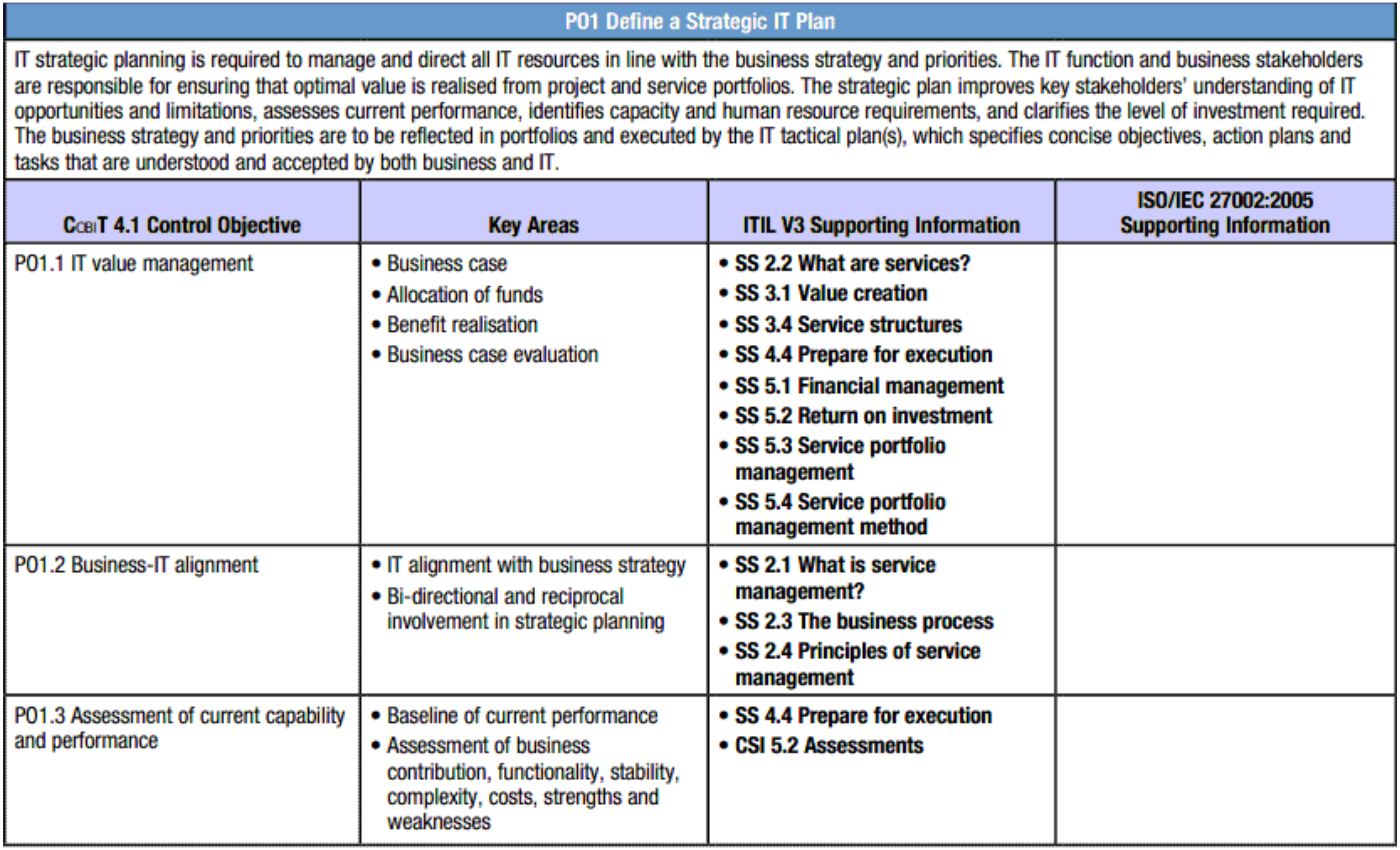
CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
ME2.1 Monitoring of internal control framework	• Continual review and improvement of internal controls		• *5.1.1 Information security policy document* • *15.2.1 Compliance with security policies and standards*
ME2.2 Supervisory review	• Review of managerial review controls		• *5.1.2 Review of the information security policy* • *6.1.8 Independent review of information security* • *10.10.2 Monitoring system use* • *10.10.4 Administrator and operator logs* • *15.2.1 Compliance with security policies and standards*
ME2.3 Control exceptions	• Analysis of control exceptions and root causes		• *15.2.1 Compliance with security policies and standards*
ME2.4 Control self-assessment	• Evaluation of controls' effectiveness through self-assessment		• *15.2.1 Compliance with security policies and standards*

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Monitor and Evaluate (ME)



ME2.5 Assurance of internal control	• Third-party reviews to provide added assurance		• *5.1.2 Review of the information security policy* • *6.1.8 Independent review of information security* • *10.10.2 Monitoring system use* • *10.10.4 Administrator and operator logs* • *15.2.1 Compliance with security policies and standards* • *15.2.2 Technical compliance checking* • *15.3.1 Information systems audit controls*
ME2.6 Internal control at third parties	• Status of external providers controls and compliance		• *6.2.3 Addressing security in third-party agreements* • *10.2.2 Monitoring and review of third-party services* • *15.2.1 Compliance with security policies and standards*
ME2.7 Remedial actions	• Remediation of control assessment exceptions		• *5.1.2 Review of the information security policy* • *15.2.1 Compliance with security policies and standards*

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Plan & Organize (PO)

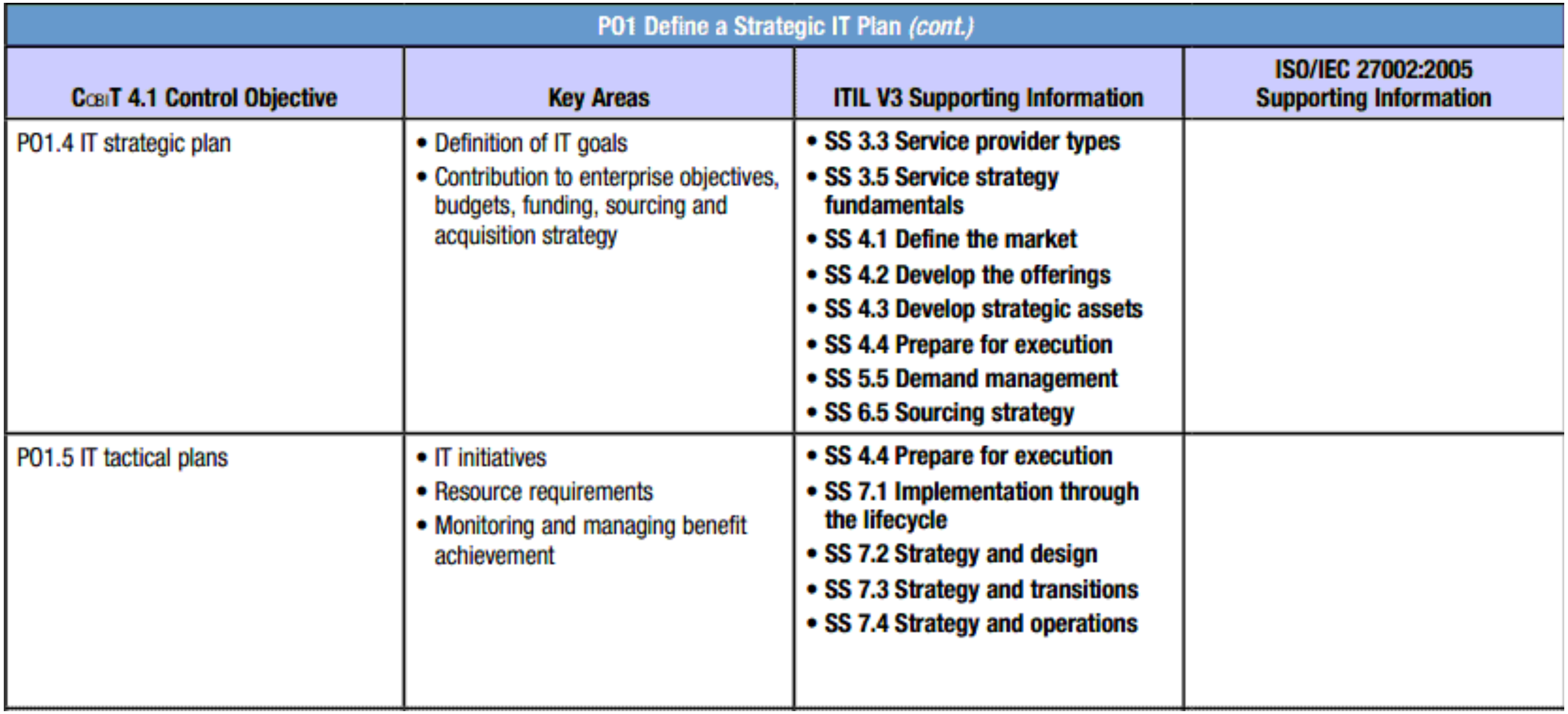


PO1 Define a Strategic IT Plan

IT strategic planning is required to manage and direct all IT resources in line with the business strategy and priorities. The IT function and business stakeholders are responsible for ensuring that optimal value is realised from project and service portfolios. The strategic plan improves key stakeholders' understanding of IT opportunities and limitations, assesses current performance, identifies capacity and human resource requirements, and clarifies the level of investment required. The business strategy and priorities are to be reflected in portfolios and executed by the IT tactical plan(s), which specifies concise objectives, action plans and tasks that are understood and accepted by both business and IT.

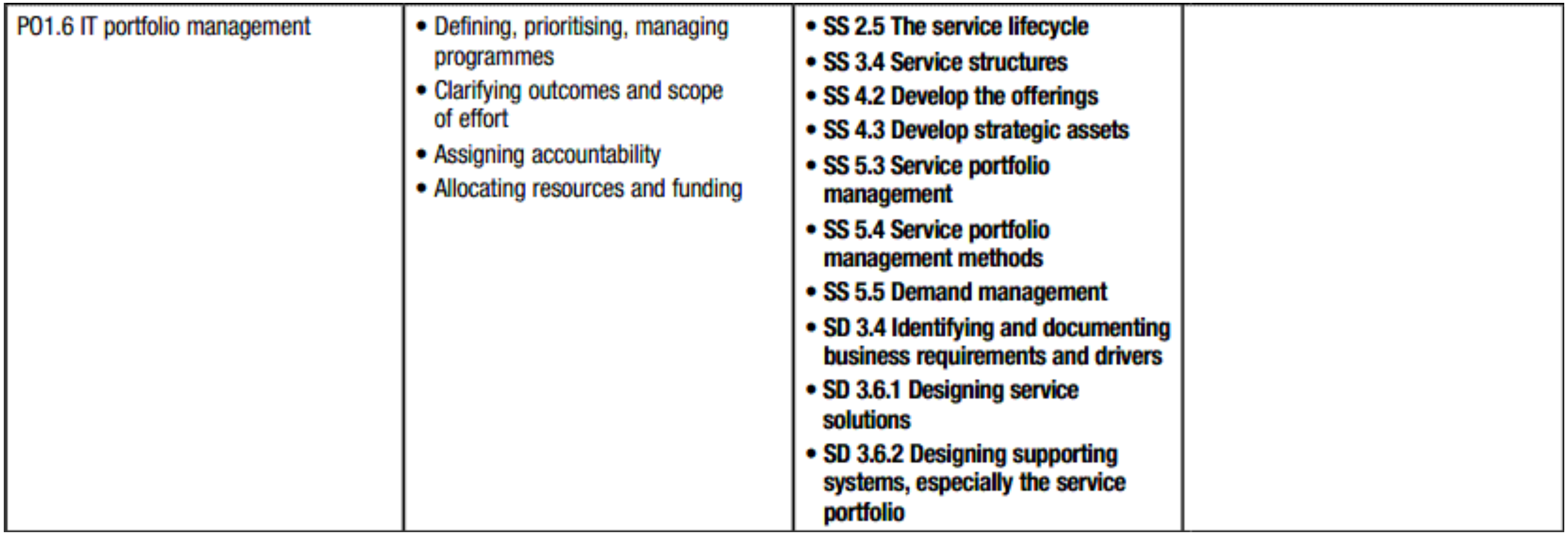
CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
PO1.1 IT value management	• Business case • Allocation of funds • Benefit realisation • Business case evaluation	• SS 2.2 What are services? • SS 3.1 Value creation • SS 3.4 Service structures • SS 4.4 Prepare for execution • SS 5.1 Financial management • SS 5.2 Return on investment • SS 5.3 Service portfolio management • SS 5.4 Service portfolio management method	
PO1.2 Business-IT alignment	• IT alignment with business strategy • Bi-directional and reciprocal involvement in strategic planning	• SS 2.1 What is service management? • SS 2.3 The business process • SS 2.4 Principles of service management	
PO1.3 Assessment of current capability and performance	• Baseline of current performance • Assessment of business contribution, functionality, stability, complexity, costs, strengths and weaknesses	• SS 4.4 Prepare for execution • CSI 5.2 Assessments	

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Plan & Organize (PO)



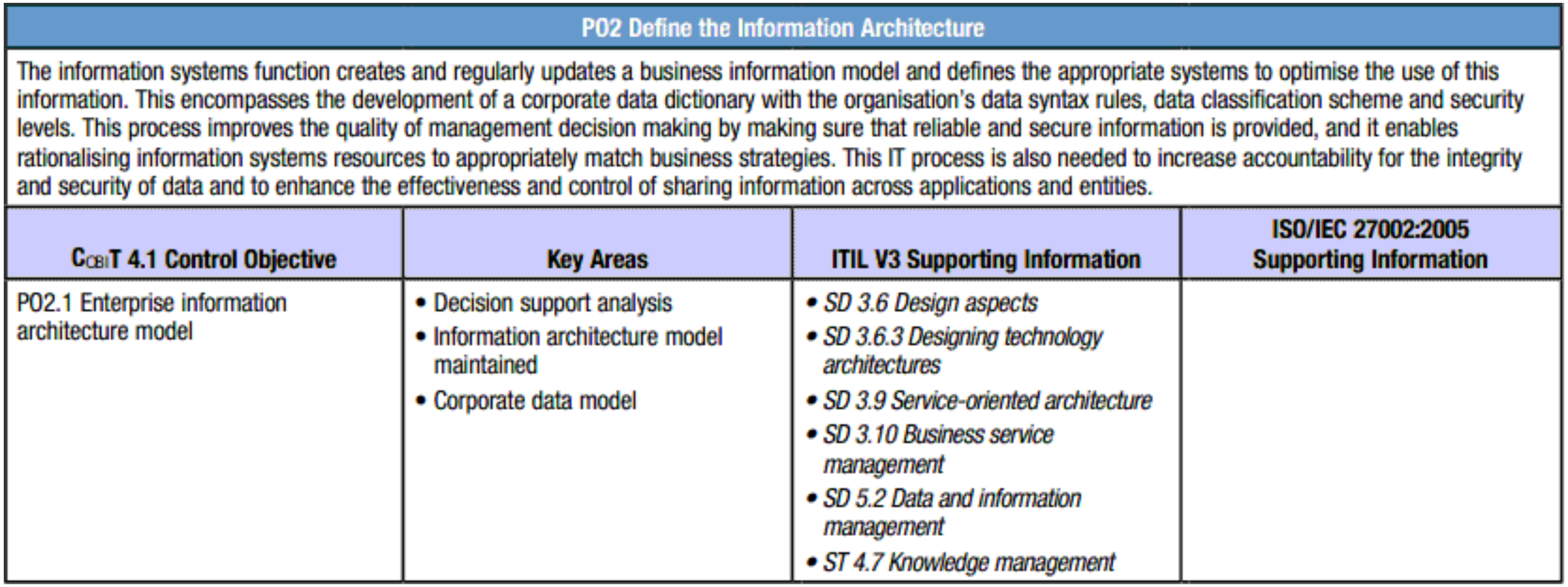
PO1 Define a Strategic IT Plan *(cont.)*			
COBIT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
PO1.4 IT strategic plan	• Definition of IT goals • Contribution to enterprise objectives, budgets, funding, sourcing and acquisition strategy	• **SS 3.3 Service provider types** • **SS 3.5 Service strategy fundamentals** • **SS 4.1 Define the market** • **SS 4.2 Develop the offerings** • **SS 4.3 Develop strategic assets** • **SS 4.4 Prepare for execution** • **SS 5.5 Demand management** • **SS 6.5 Sourcing strategy**	
PO1.5 IT tactical plans	• IT initiatives • Resource requirements • Monitoring and managing benefit achievement	• **SS 4.4 Prepare for execution** • **SS 7.1 Implementation through the lifecycle** • **SS 7.2 Strategy and design** • **SS 7.3 Strategy and transitions** • **SS 7.4 Strategy and operations**	

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Plan & Organize (PO)



P01.6 IT portfolio management	• Defining, prioritising, managing programmes • Clarifying outcomes and scope of effort • Assigning accountability • Allocating resources and funding	**• SS 2.5 The service lifecycle • SS 3.4 Service structures • SS 4.2 Develop the offerings • SS 4.3 Develop strategic assets • SS 5.3 Service portfolio management • SS 5.4 Service portfolio management methods • SS 5.5 Demand management • SD 3.4 Identifying and documenting business requirements and drivers • SD 3.6.1 Designing service solutions • SD 3.6.2 Designing supporting systems, especially the service portfolio**	

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Plan & Organize (PO)

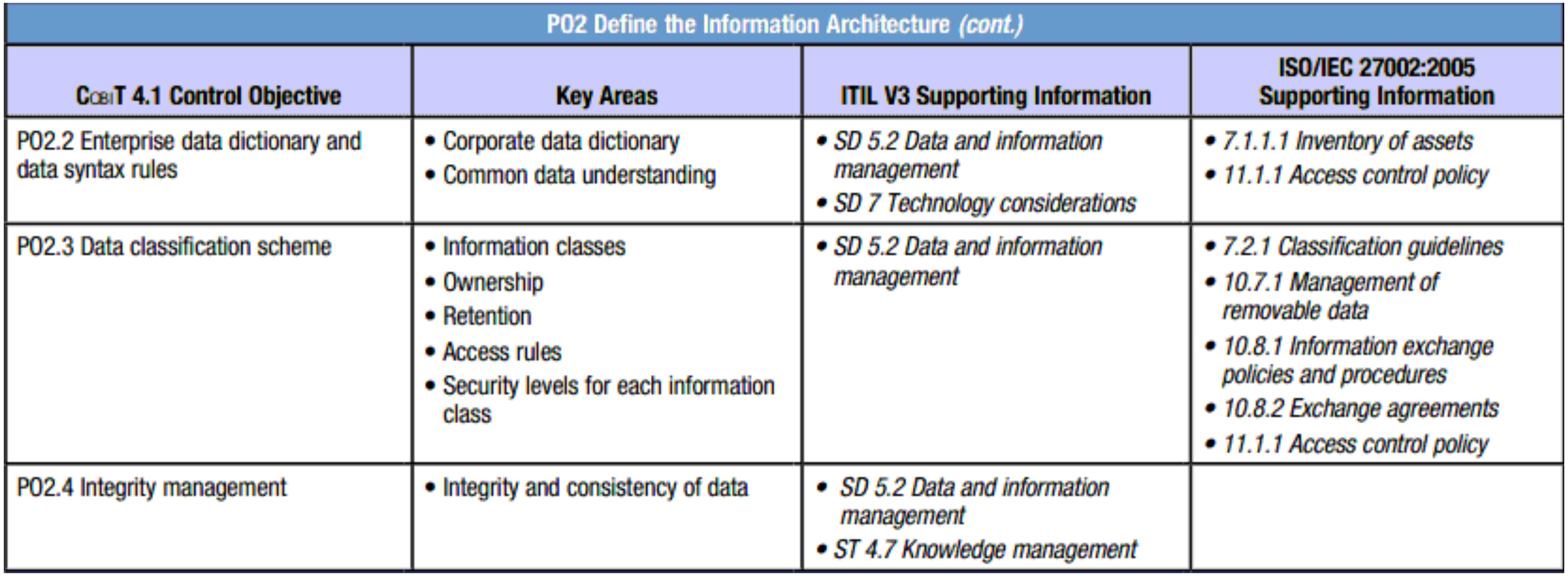


PO2 Define the Information Architecture

The information systems function creates and regularly updates a business information model and defines the appropriate systems to optimise the use of this information. This encompasses the development of a corporate data dictionary with the organisation's data syntax rules, data classification scheme and security levels. This process improves the quality of management decision making by making sure that reliable and secure information is provided, and it enables rationalising information systems resources to appropriately match business strategies. This IT process is also needed to increase accountability for the integrity and security of data and to enhance the effectiveness and control of sharing information across applications and entities.

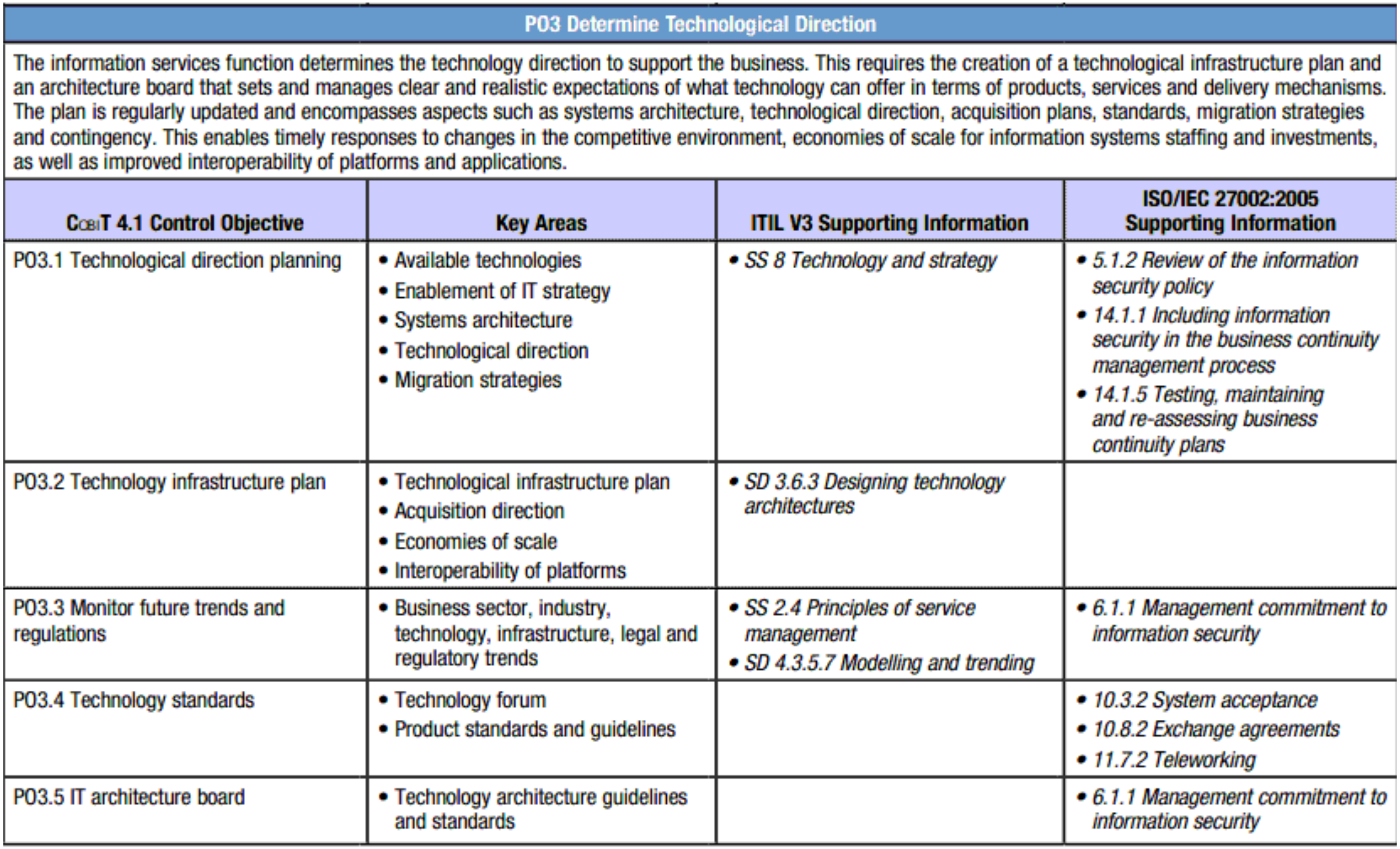
CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
PO2.1 Enterprise information architecture model	• Decision support analysis • Information architecture model maintained • Corporate data model	• *SD 3.6 Design aspects* • *SD 3.6.3 Designing technology architectures* • *SD 3.9 Service-oriented architecture* • *SD 3.10 Business service management* • *SD 5.2 Data and information management* • *ST 4.7 Knowledge management*	

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Plan & Organize (PO)



PO2 Define the Information Architecture *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
PO2.2 Enterprise data dictionary and data syntax rules	• Corporate data dictionary • Common data understanding	• *SD 5.2 Data and information management* • *SD 7 Technology considerations*	• *7.1.1.1 Inventory of assets* • *11.1.1 Access control policy*
PO2.3 Data classification scheme	• Information classes • Ownership • Retention • Access rules • Security levels for each information class	• *SD 5.2 Data and information management*	• *7.2.1 Classification guidelines* • *10.7.1 Management of removable data* • *10.8.1 Information exchange policies and procedures* • *10.8.2 Exchange agreements* • *11.1.1 Access control policy*
PO2.4 Integrity management	• Integrity and consistency of data	• *SD 5.2 Data and information management* • *ST 4.7 Knowledge management*	

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Plan & Organize (PO)

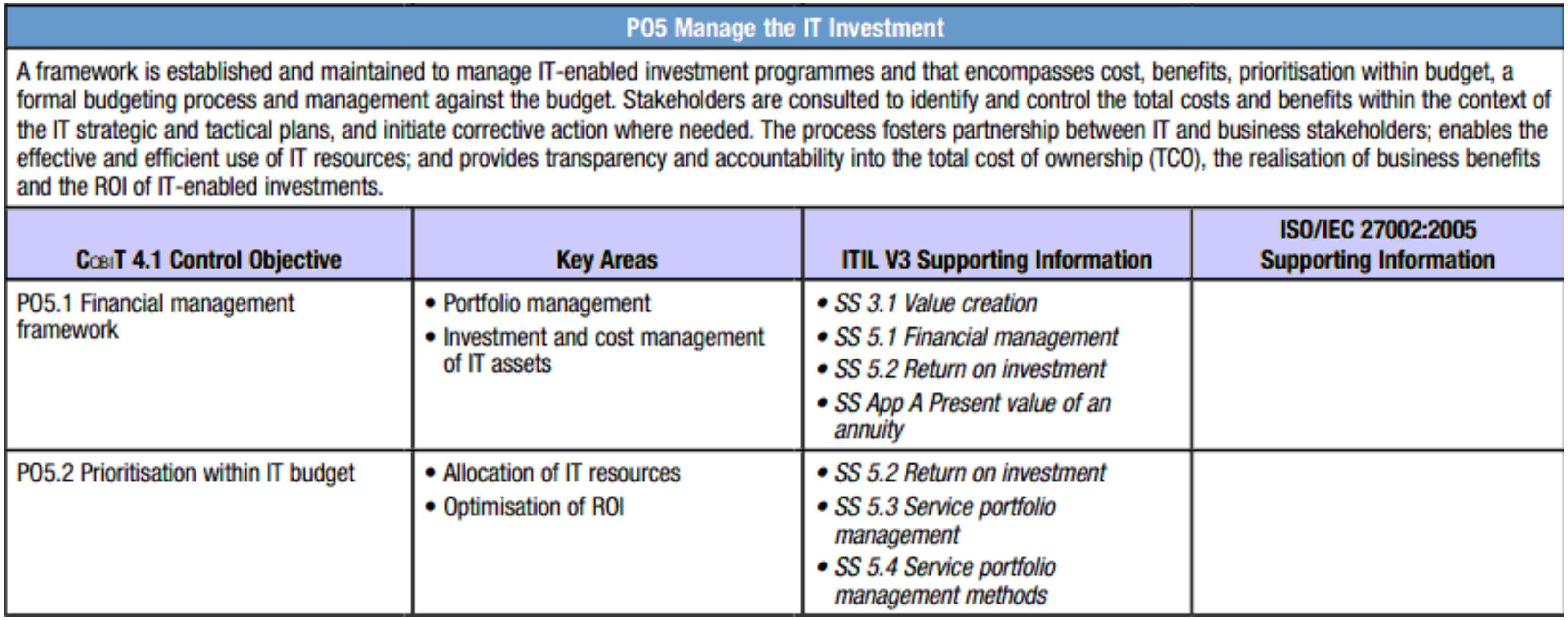


PO3 Determine Technological Direction

The information services function determines the technology direction to support the business. This requires the creation of a technological infrastructure plan and an architecture board that sets and manages clear and realistic expectations of what technology can offer in terms of products, services and delivery mechanisms. The plan is regularly updated and encompasses aspects such as systems architecture, technological direction, acquisition plans, standards, migration strategies and contingency. This enables timely responses to changes in the competitive environment, economies of scale for information systems staffing and investments, as well as improved interoperability of platforms and applications.

CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
PO3.1 Technological direction planning	• Available technologies • Enablement of IT strategy • Systems architecture • Technological direction • Migration strategies	• *SS 8 Technology and strategy*	• *5.1.2 Review of the information security policy* • *14.1.1 Including information security in the business continuity management process* • *14.1.5 Testing, maintaining and re-assessing business continuity plans*
PO3.2 Technology infrastructure plan	• Technological infrastructure plan • Acquisition direction • Economies of scale • Interoperability of platforms	• *SD 3.6.3 Designing technology architectures*	
PO3.3 Monitor future trends and regulations	• Business sector, industry, technology, infrastructure, legal and regulatory trends	• *SS 2.4 Principles of service management* • *SD 4.3.5.7 Modelling and trending*	• *6.1.1 Management commitment to information security*
PO3.4 Technology standards	• Technology forum • Product standards and guidelines		• *10.3.2 System acceptance* • *10.8.2 Exchange agreements* • *11.7.2 Teleworking*
PO3.5 IT architecture board	• Technology architecture guidelines and standards		• *6.1.1 Management commitment to information security*

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Plan & Organize (PO)

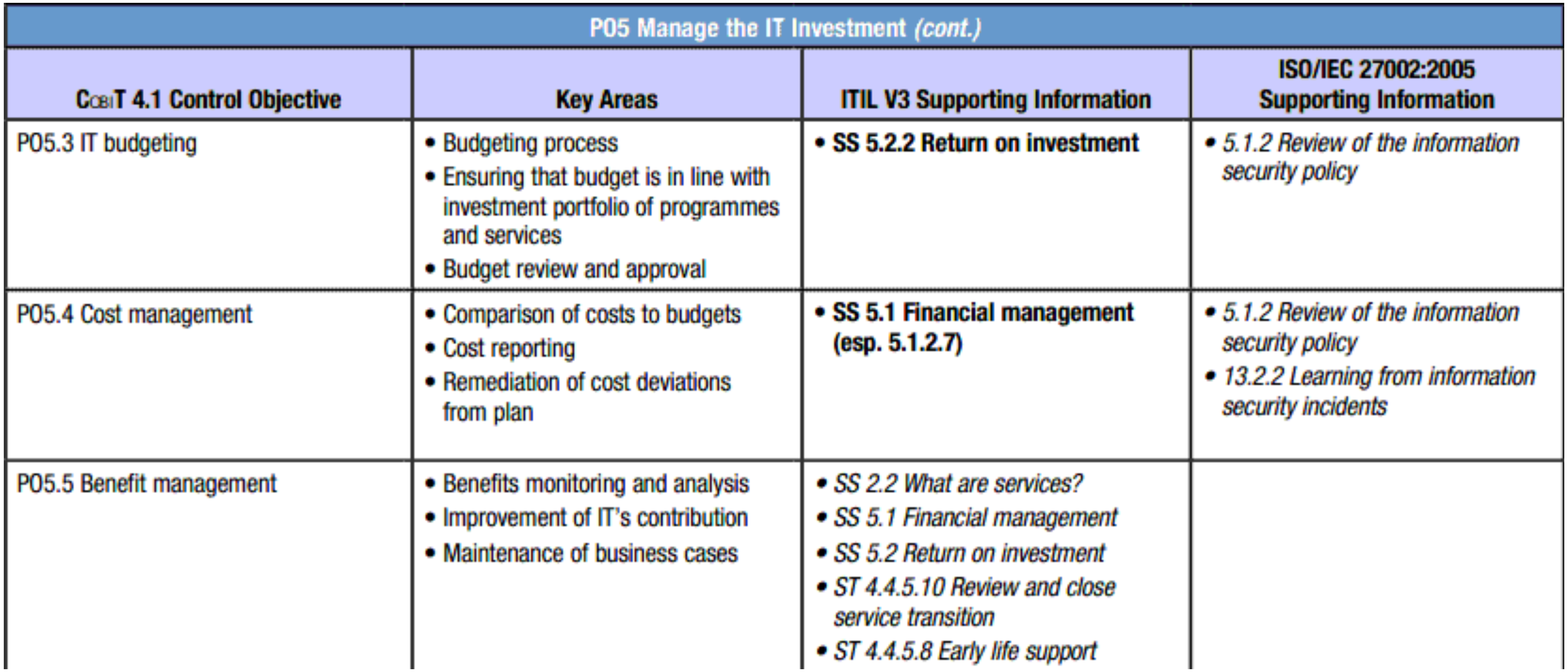


PO5 Manage the IT Investment

A framework is established and maintained to manage IT-enabled investment programmes and that encompasses cost, benefits, prioritisation within budget, a formal budgeting process and management against the budget. Stakeholders are consulted to identify and control the total costs and benefits within the context of the IT strategic and tactical plans, and initiate corrective action where needed. The process fosters partnership between IT and business stakeholders; enables the effective and efficient use of IT resources; and provides transparency and accountability into the total cost of ownership (TCO), the realisation of business benefits and the ROI of IT-enabled investments.

CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
PO5.1 Financial management framework	• Portfolio management • Investment and cost management of IT assets	• *SS 3.1 Value creation* • *SS 5.1 Financial management* • *SS 5.2 Return on investment* • *SS App A Present value of an annuity*	
PO5.2 Prioritisation within IT budget	• Allocation of IT resources • Optimisation of ROI	• *SS 5.2 Return on investment* • *SS 5.3 Service portfolio management* • *SS 5.4 Service portfolio management methods*	

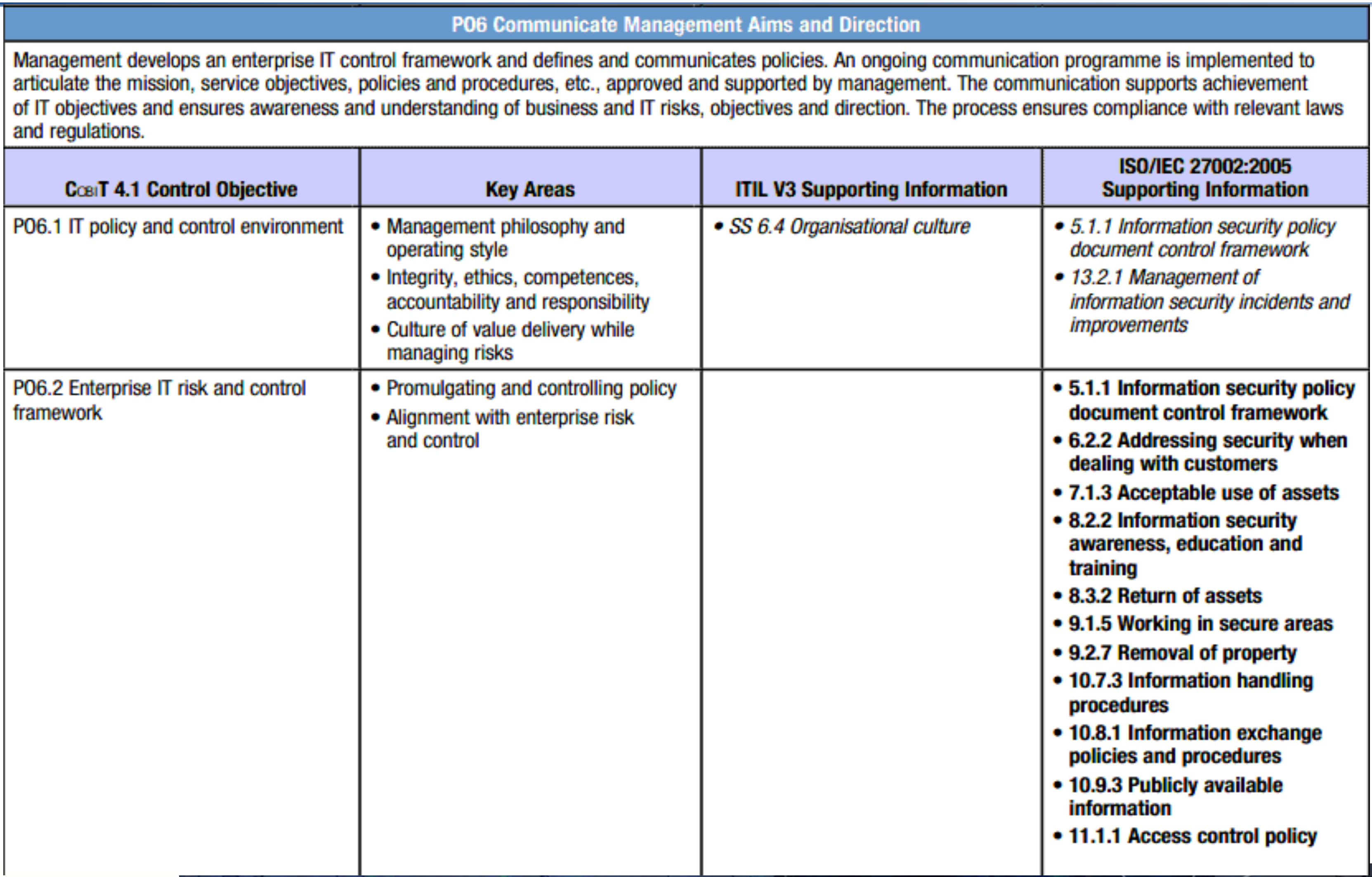
Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Plan & Organize (PO)



PO5 Manage the IT Investment *(cont.)*

CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
PO5.3 IT budgeting	• Budgeting process • Ensuring that budget is in line with investment portfolio of programmes and services • Budget review and approval	**• SS 5.2.2 Return on investment**	*• 5.1.2 Review of the information security policy*
PO5.4 Cost management	• Comparison of costs to budgets • Cost reporting • Remediation of cost deviations from plan	**• SS 5.1 Financial management (esp. 5.1.2.7)**	*• 5.1.2 Review of the information security policy* *• 13.2.2 Learning from information security incidents*
PO5.5 Benefit management	• Benefits monitoring and analysis • Improvement of IT's contribution • Maintenance of business cases	*• SS 2.2 What are services?* *• SS 5.1 Financial management* *• SS 5.2 Return on investment* *• ST 4.4.5.10 Review and close service transition* *• ST 4.4.5.8 Early life support*	

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Plan & Organize (PO)

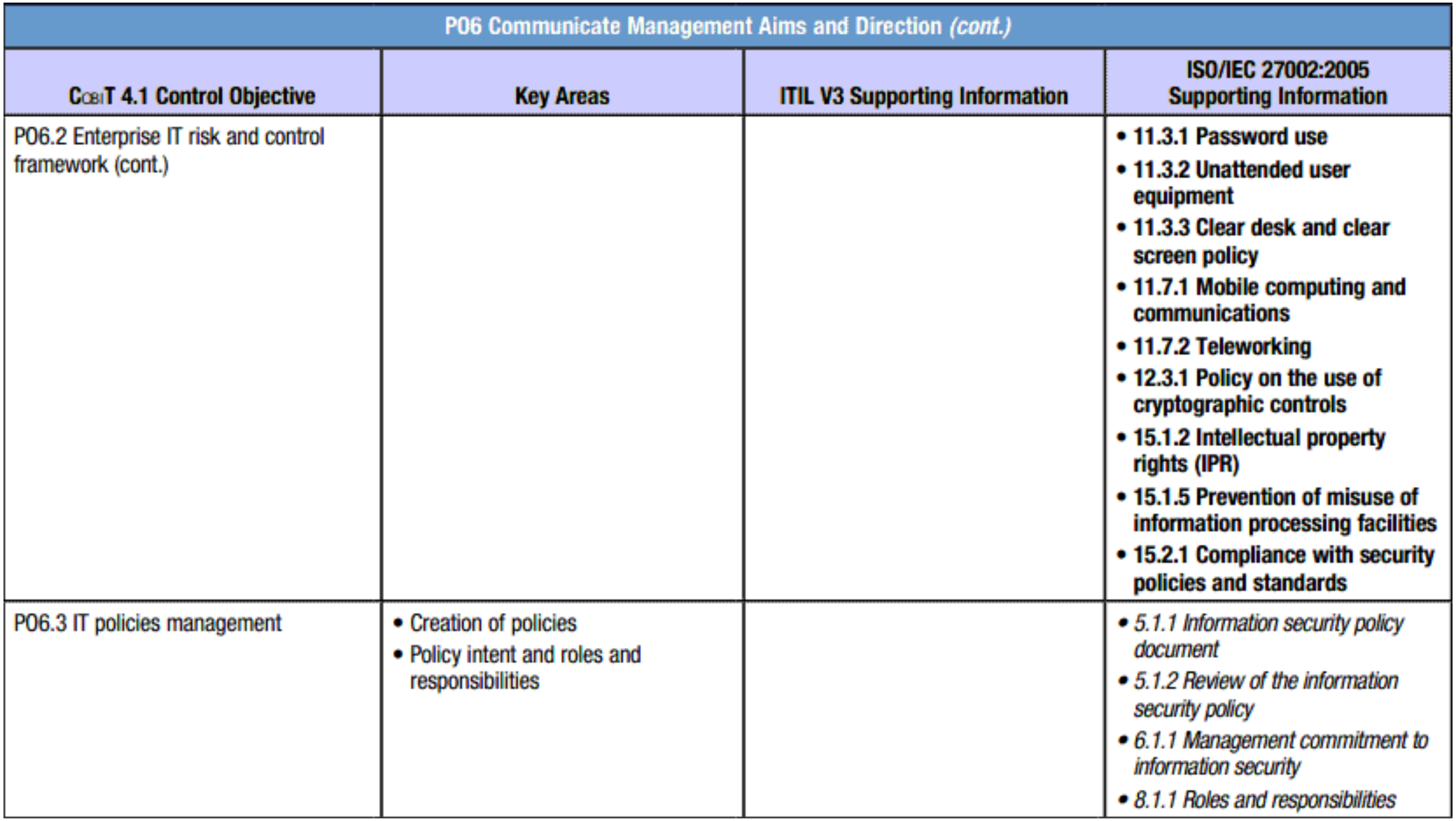


PO6 Communicate Management Aims and Direction

Management develops an enterprise IT control framework and defines and communicates policies. An ongoing communication programme is implemented to articulate the mission, service objectives, policies and procedures, etc., approved and supported by management. The communication supports achievement of IT objectives and ensures awareness and understanding of business and IT risks, objectives and direction. The process ensures compliance with relevant laws and regulations.

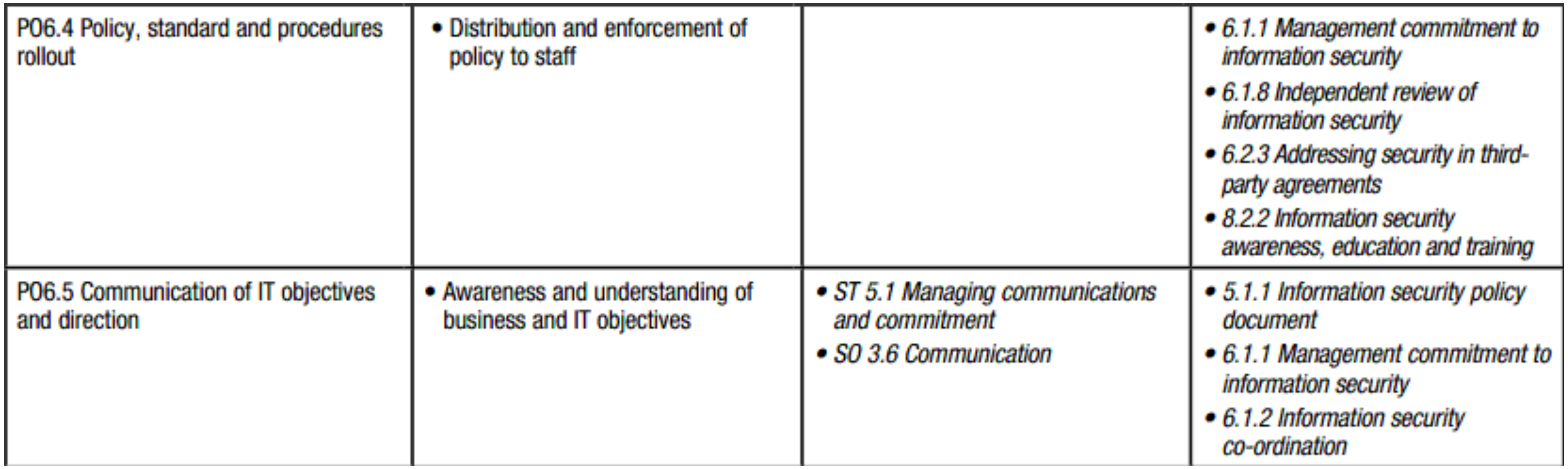
CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
PO6.1 IT policy and control environment	• Management philosophy and operating style • Integrity, ethics, competences, accountability and responsibility • Culture of value delivery while managing risks	• *SS 6.4 Organisational culture*	• *5.1.1 Information security policy document control framework* • *13.2.1 Management of information security incidents and improvements*
PO6.2 Enterprise IT risk and control framework	• Promulgating and controlling policy • Alignment with enterprise risk and control		• **5.1.1 Information security policy document control framework** • **6.2.2 Addressing security when dealing with customers** • **7.1.3 Acceptable use of assets** • **8.2.2 Information security awareness, education and training** • **8.3.2 Return of assets** • **9.1.5 Working in secure areas** • **9.2.7 Removal of property** • **10.7.3 Information handling procedures** • **10.8.1 Information exchange policies and procedures** • **10.9.3 Publicly available information** • **11.1.1 Access control policy**

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Plan & Organize (PO)



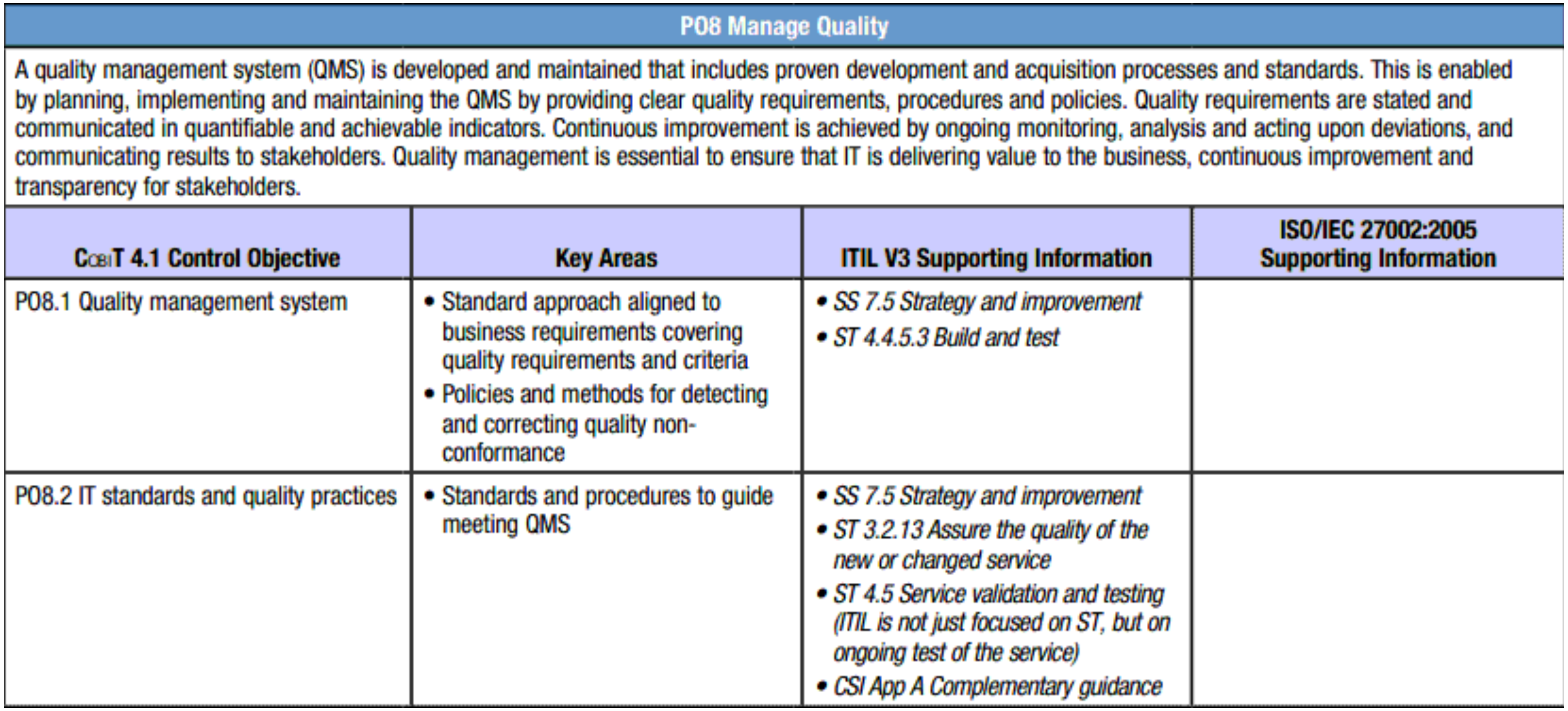
PO6 Communicate Management Aims and Direction *(cont.)*			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
PO6.2 Enterprise IT risk and control framework (cont.)			• 11.3.1 Password use • 11.3.2 Unattended user equipment • 11.3.3 Clear desk and clear screen policy • 11.7.1 Mobile computing and communications • 11.7.2 Teleworking • 12.3.1 Policy on the use of cryptographic controls • 15.1.2 Intellectual property rights (IPR) • 15.1.5 Prevention of misuse of information processing facilities • 15.2.1 Compliance with security policies and standards
PO6.3 IT policies management	• Creation of policies • Policy intent and roles and responsibilities		• *5.1.1 Information security policy document* • *5.1.2 Review of the information security policy* • *6.1.1 Management commitment to information security* • *8.1.1 Roles and responsibilities*

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Plan & Organize (PO)



PO6.4 Policy, standard and procedures rollout	• Distribution and enforcement of policy to staff		• *6.1.1 Management commitment to information security* • *6.1.8 Independent review of information security* • *6.2.3 Addressing security in third-party agreements* • *8.2.2 Information security awareness, education and training*
PO6.5 Communication of IT objectives and direction	• Awareness and understanding of business and IT objectives	• *ST 5.1 Managing communications and commitment* • *SO 3.6 Communication*	• *5.1.1 Information security policy document* • *6.1.1 Management commitment to information security* • *6.1.2 Information security co-ordination*

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Plan & Organize (PO)

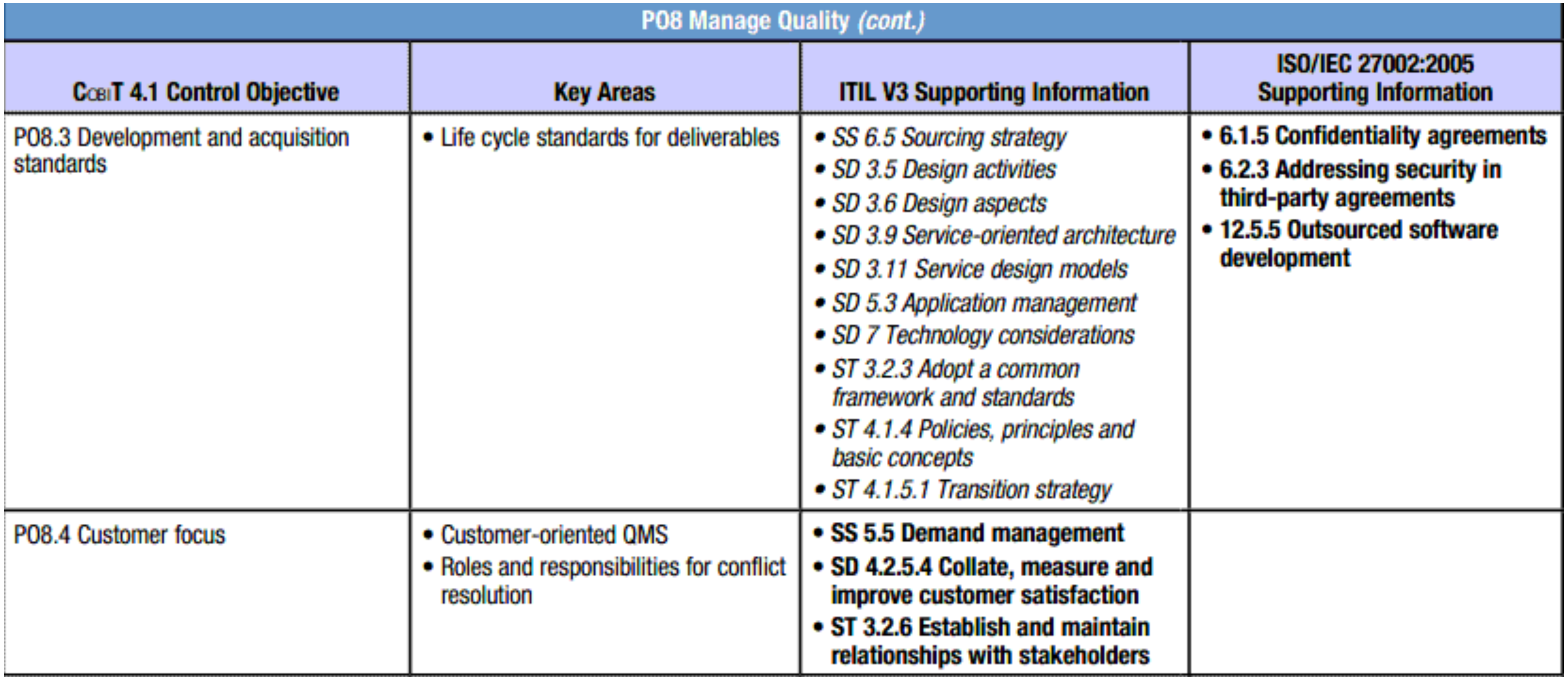


PO8 Manage Quality

A quality management system (QMS) is developed and maintained that includes proven development and acquisition processes and standards. This is enabled by planning, implementing and maintaining the QMS by providing clear quality requirements, procedures and policies. Quality requirements are stated and communicated in quantifiable and achievable indicators. Continuous improvement is achieved by ongoing monitoring, analysis and acting upon deviations, and communicating results to stakeholders. Quality management is essential to ensure that IT is delivering value to the business, continuous improvement and transparency for stakeholders.

COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
PO8.1 Quality management system	• Standard approach aligned to business requirements covering quality requirements and criteria • Policies and methods for detecting and correcting quality non-conformance	• *SS 7.5 Strategy and improvement* • *ST 4.4.5.3 Build and test*	
PO8.2 IT standards and quality practices	• Standards and procedures to guide meeting QMS	• *SS 7.5 Strategy and improvement* • *ST 3.2.13 Assure the quality of the new or changed service* • *ST 4.5 Service validation and testing (ITIL is not just focused on ST, but on ongoing test of the service)* • *CSI App A Complementary guidance*	

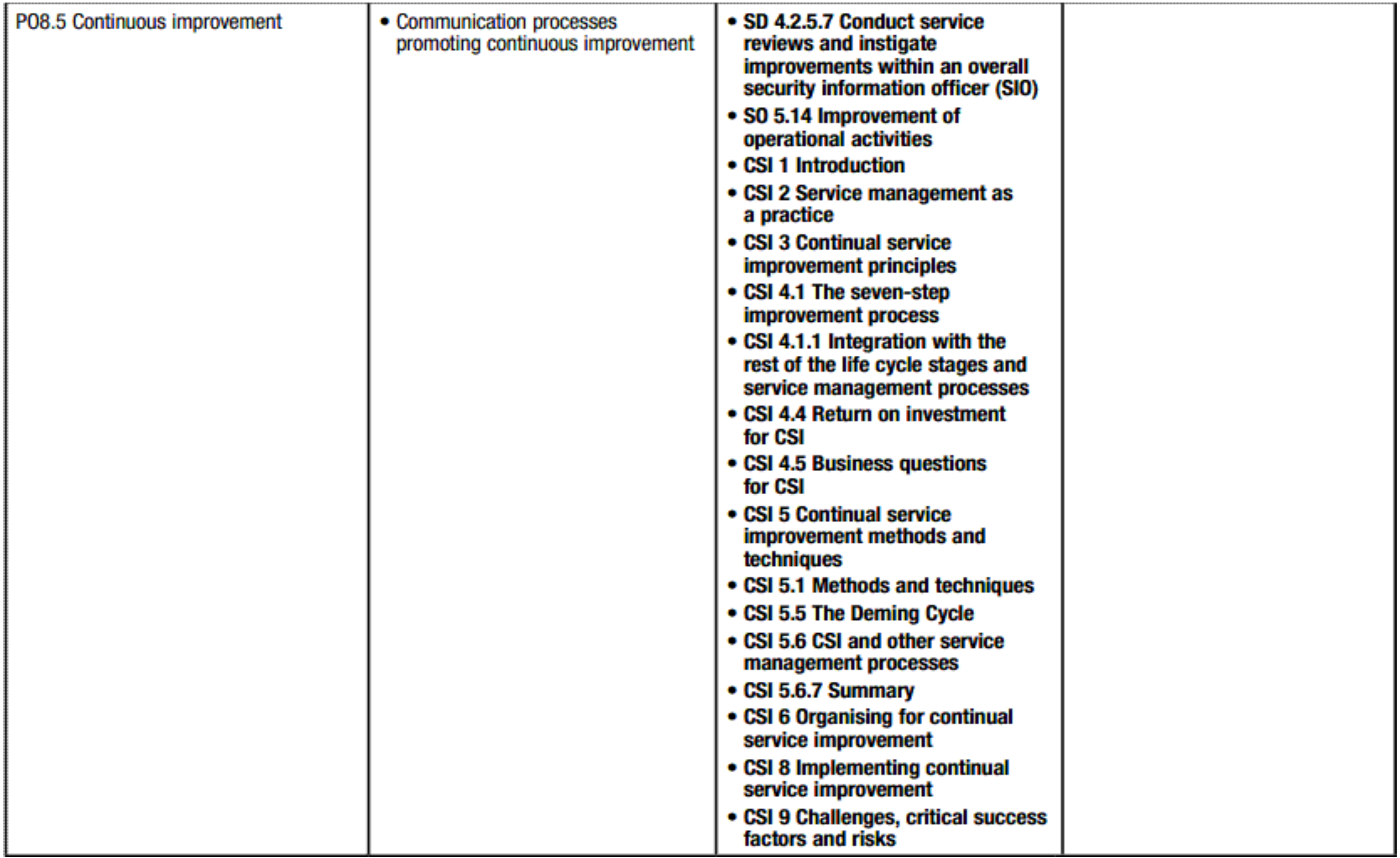
Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Plan & Organize (PO)



PO8 Manage Quality *(cont.)*

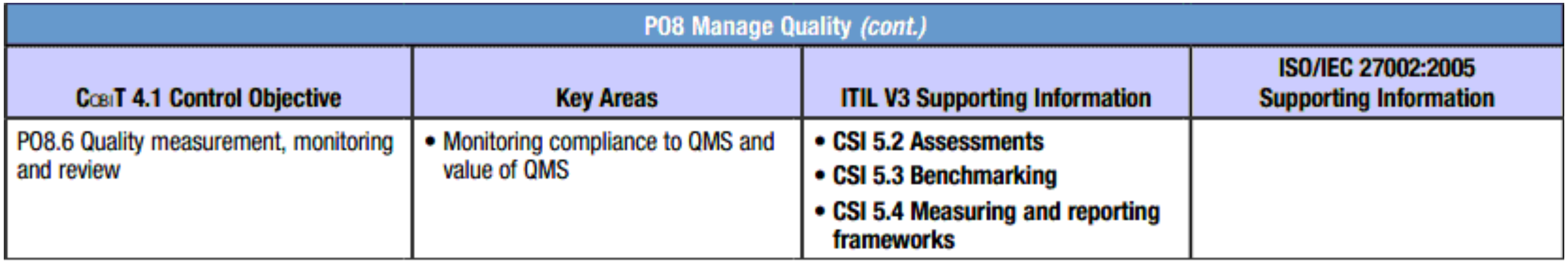
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
PO8.3 Development and acquisition standards	• Life cycle standards for deliverables	• *SS 6.5 Sourcing strategy* • *SD 3.5 Design activities* • *SD 3.6 Design aspects* • *SD 3.9 Service-oriented architecture* • *SD 3.11 Service design models* • *SD 5.3 Application management* • *SD 7 Technology considerations* • *ST 3.2.3 Adopt a common framework and standards* • *ST 4.1.4 Policies, principles and basic concepts* • *ST 4.1.5.1 Transition strategy*	• **6.1.5 Confidentiality agreements** • **6.2.3 Addressing security in third-party agreements** • **12.5.5 Outsourced software development**
PO8.4 Customer focus	• Customer-oriented QMS • Roles and responsibilities for conflict resolution	• **SS 5.5 Demand management** • **SD 4.2.5.4 Collate, measure and improve customer satisfaction** • **ST 3.2.6 Establish and maintain relationships with stakeholders**	

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Plan & Organize (PO)



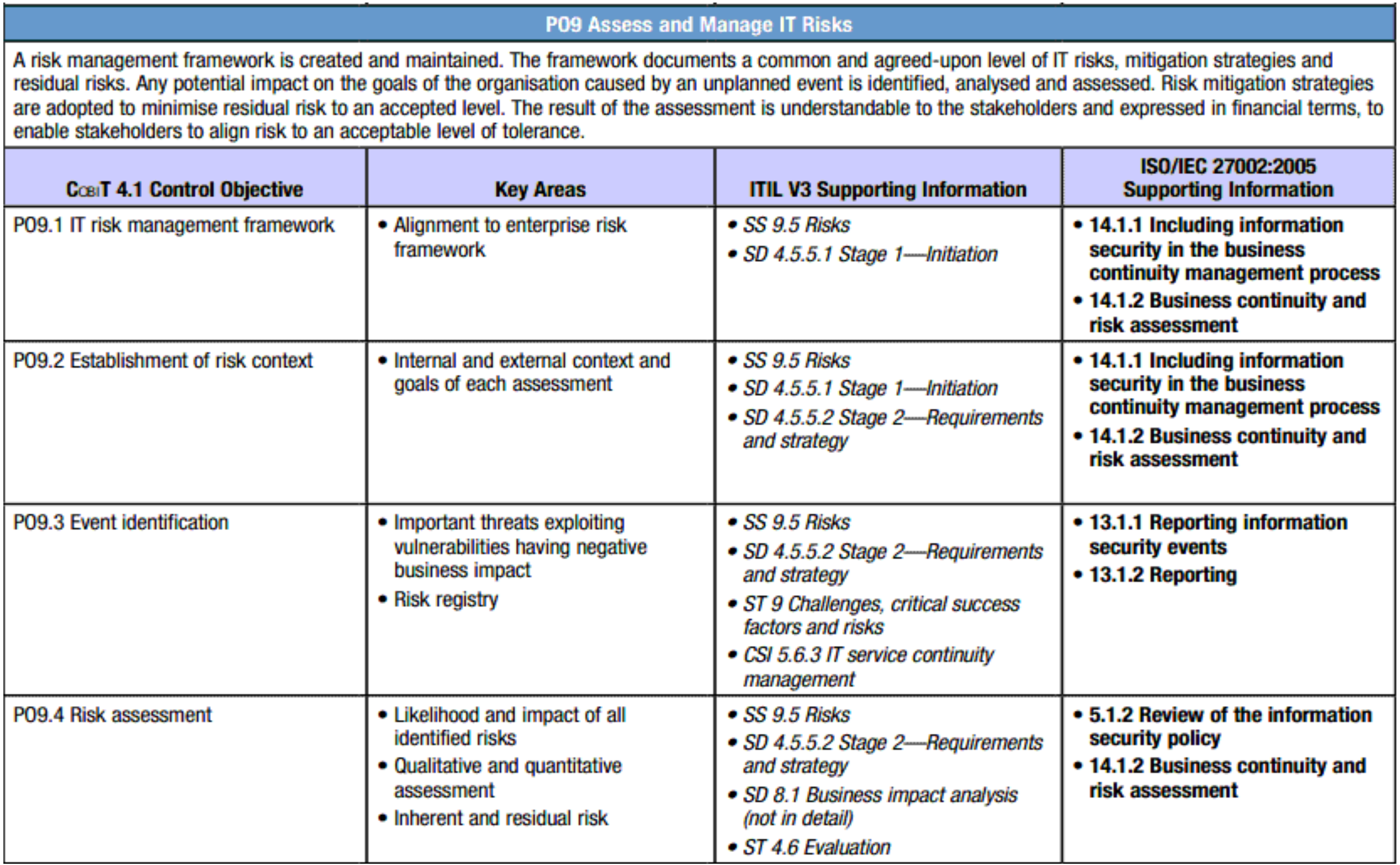
PO8.5 Continuous improvement	• Communication processes promoting continuous improvement	• SD 4.2.5.7 Conduct service reviews and instigate improvements within an overall security information officer (SIO) • SO 5.14 Improvement of operational activities • CSI 1 Introduction • CSI 2 Service management as a practice • CSI 3 Continual service improvement principles • CSI 4.1 The seven-step improvement process • CSI 4.1.1 Integration with the rest of the life cycle stages and service management processes • CSI 4.4 Return on investment for CSI • CSI 4.5 Business questions for CSI • CSI 5 Continual service improvement methods and techniques • CSI 5.1 Methods and techniques • CSI 5.5 The Deming Cycle • CSI 5.6 CSI and other service management processes • CSI 5.6.7 Summary • CSI 6 Organising for continual service improvement • CSI 8 Implementing continual service improvement • CSI 9 Challenges, critical success factors and risks	

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Plan & Organize (PO)



PO8 Manage Quality *(cont.)*			
CobiT 4.1 Control Objective	**Key Areas**	**ITIL V3 Supporting Information**	**ISO/IEC 27002:2005 Supporting Information**
PO8.6 Quality measurement, monitoring and review	• Monitoring compliance to QMS and value of QMS	• **CSI 5.2 Assessments** • **CSI 5.3 Benchmarking** • **CSI 5.4 Measuring and reporting frameworks**	

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Plan & Organize (PO)

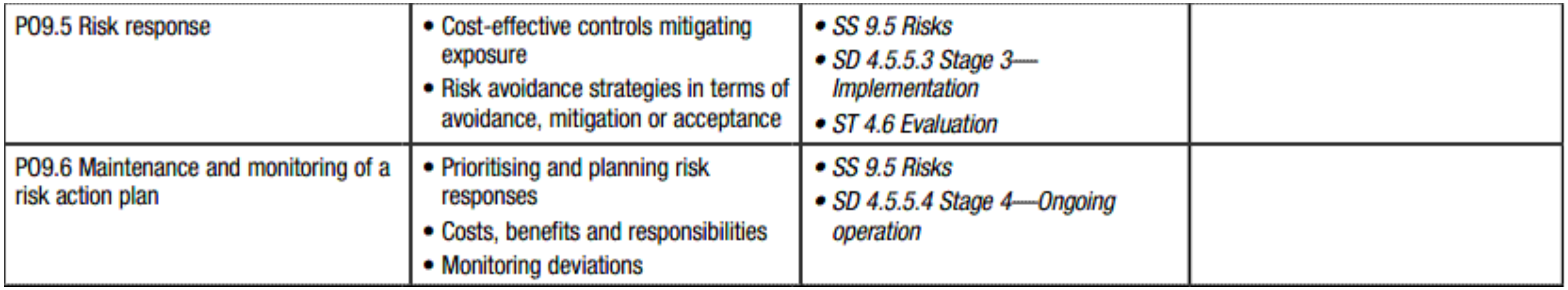


PO9 Assess and Manage IT Risks

A risk management framework is created and maintained. The framework documents a common and agreed-upon level of IT risks, mitigation strategies and residual risks. Any potential impact on the goals of the organisation caused by an unplanned event is identified, analysed and assessed. Risk mitigation strategies are adopted to minimise residual risk to an accepted level. The result of the assessment is understandable to the stakeholders and expressed in financial terms, to enable stakeholders to align risk to an acceptable level of tolerance.

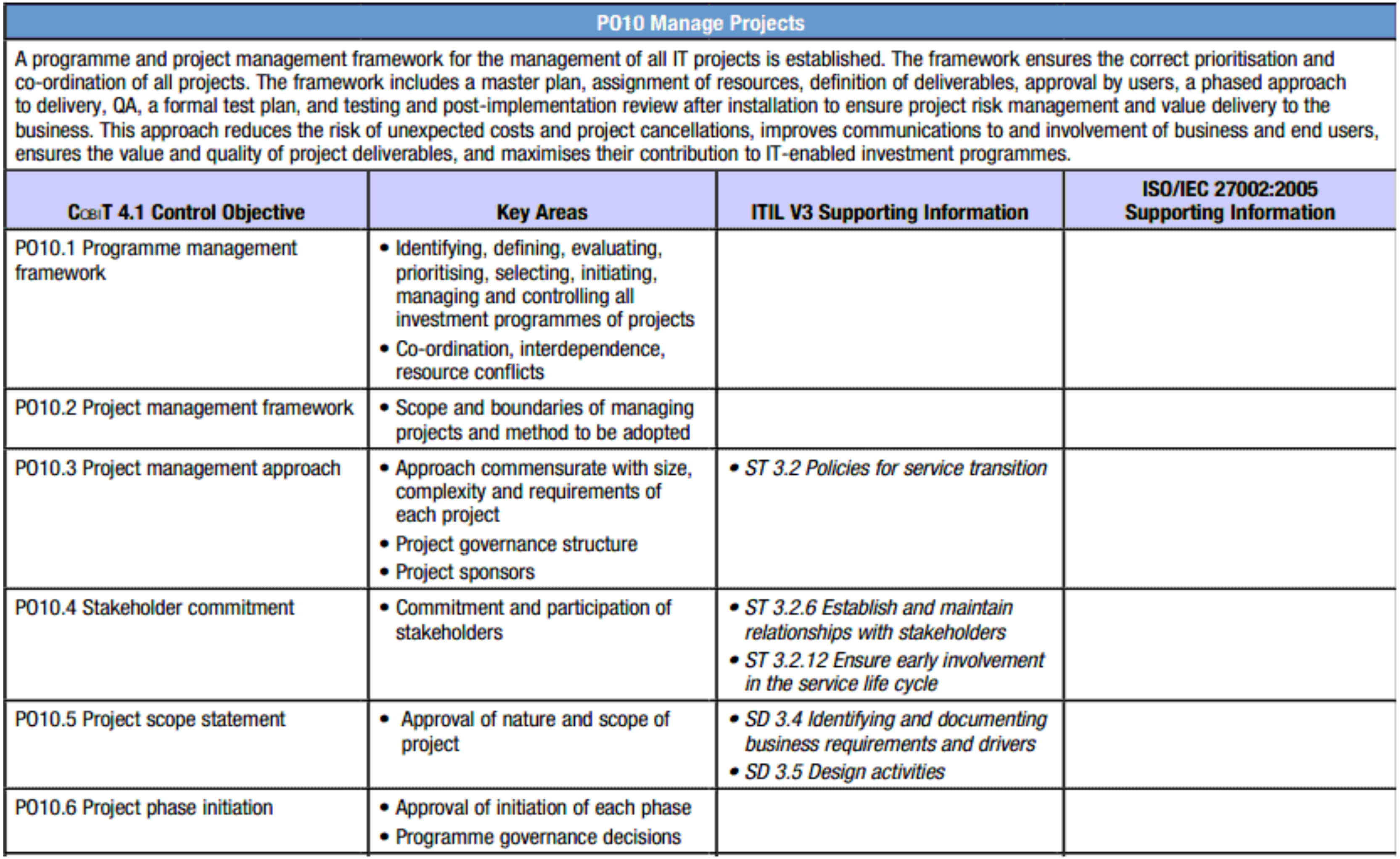
CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
PO9.1 IT risk management framework	• Alignment to enterprise risk framework	• *SS 9.5 Risks* • *SD 4.5.5.1 Stage 1—Initiation*	• **14.1.1 Including information security in the business continuity management process** • **14.1.2 Business continuity and risk assessment**
PO9.2 Establishment of risk context	• Internal and external context and goals of each assessment	• *SS 9.5 Risks* • *SD 4.5.5.1 Stage 1—Initiation* • *SD 4.5.5.2 Stage 2—Requirements and strategy*	• **14.1.1 Including information security in the business continuity management process** • **14.1.2 Business continuity and risk assessment**
PO9.3 Event identification	• Important threats exploiting vulnerabilities having negative business impact • Risk registry	• *SS 9.5 Risks* • *SD 4.5.5.2 Stage 2—Requirements and strategy* • *ST 9 Challenges, critical success factors and risks* • *CSI 5.6.3 IT service continuity management*	• **13.1.1 Reporting information security events** • **13.1.2 Reporting**
PO9.4 Risk assessment	• Likelihood and impact of all identified risks • Qualitative and quantitative assessment • Inherent and residual risk	• *SS 9.5 Risks* • *SD 4.5.5.2 Stage 2—Requirements and strategy* • *SD 8.1 Business impact analysis (not in detail)* • *ST 4.6 Evaluation*	• **5.1.2 Review of the information security policy** • **14.1.2 Business continuity and risk assessment**

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Plan & Organize (PO)



PO9.5 Risk response	• Cost-effective controls mitigating exposure • Risk avoidance strategies in terms of avoidance, mitigation or acceptance	• *SS 9.5 Risks* • *SD 4.5.5.3 Stage 3—Implementation* • *ST 4.6 Evaluation*	
PO9.6 Maintenance and monitoring of a risk action plan	• Prioritising and planning risk responses • Costs, benefits and responsibilities • Monitoring deviations	• *SS 9.5 Risks* • *SD 4.5.5.4 Stage 4—Ongoing operation*	

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Plan & Organize (PO)

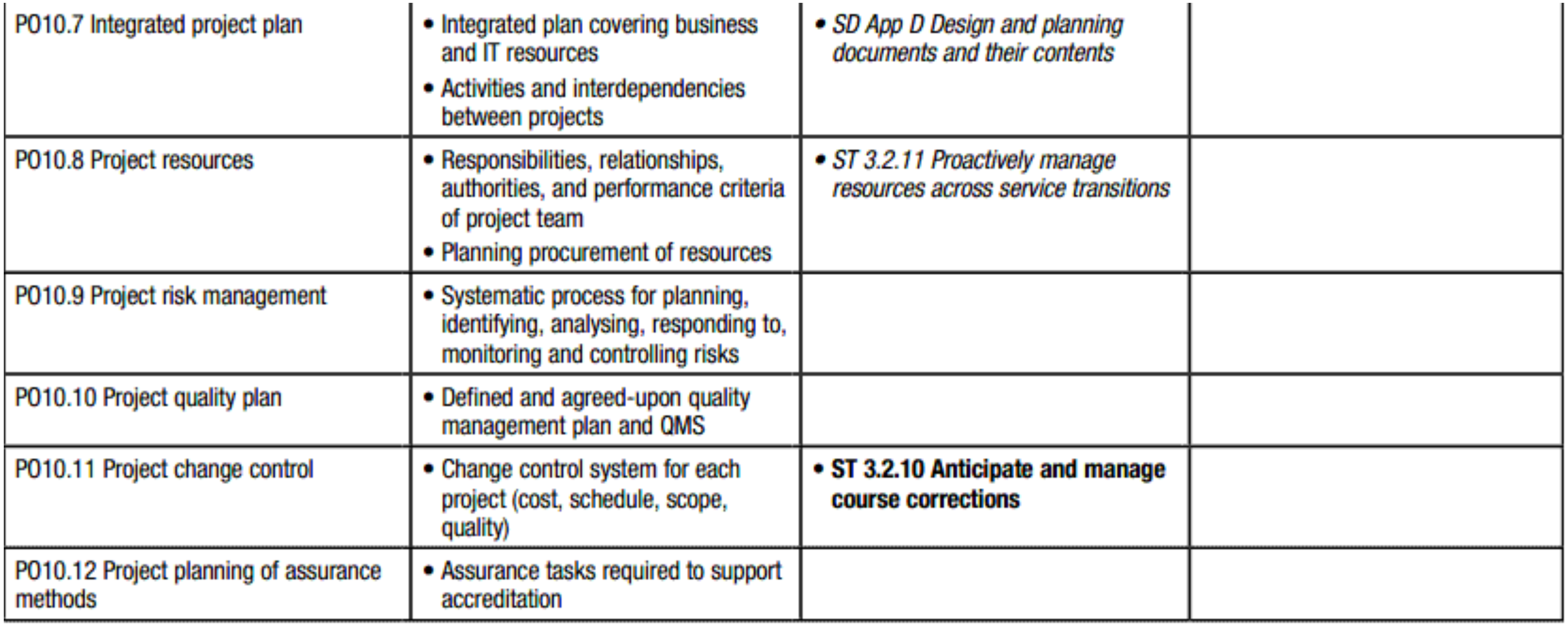


PO10 Manage Projects

A programme and project management framework for the management of all IT projects is established. The framework ensures the correct prioritisation and co-ordination of all projects. The framework includes a master plan, assignment of resources, definition of deliverables, approval by users, a phased approach to delivery, QA, a formal test plan, and testing and post-implementation review after installation to ensure project risk management and value delivery to the business. This approach reduces the risk of unexpected costs and project cancellations, improves communications to and involvement of business and end users, ensures the value and quality of project deliverables, and maximises their contribution to IT-enabled investment programmes.

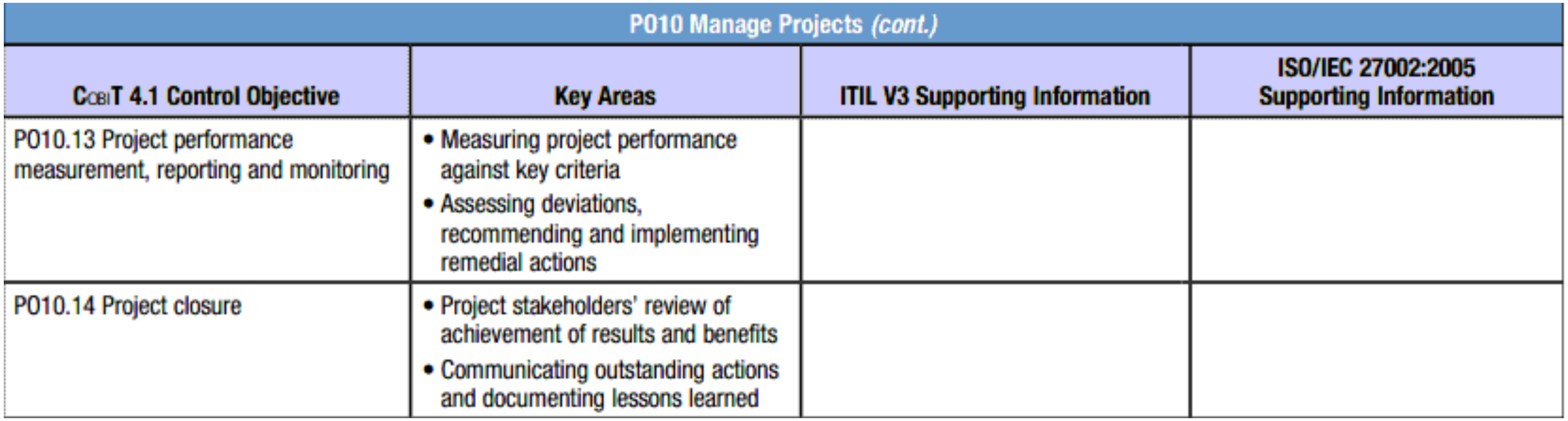
CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
PO10.1 Programme management framework	• Identifying, defining, evaluating, prioritising, selecting, initiating, managing and controlling all investment programmes of projects • Co-ordination, interdependence, resource conflicts		
PO10.2 Project management framework	• Scope and boundaries of managing projects and method to be adopted		
PO10.3 Project management approach	• Approach commensurate with size, complexity and requirements of each project • Project governance structure • Project sponsors	• *ST 3.2 Policies for service transition*	
PO10.4 Stakeholder commitment	• Commitment and participation of stakeholders	• *ST 3.2.6 Establish and maintain relationships with stakeholders* • *ST 3.2.12 Ensure early involvement in the service life cycle*	
PO10.5 Project scope statement	• Approval of nature and scope of project	• *SD 3.4 Identifying and documenting business requirements and drivers* • *SD 3.5 Design activities*	
PO10.6 Project phase initiation	• Approval of initiation of each phase • Programme governance decisions		

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Plan & Organize (PO)



PO10.7 Integrated project plan	• Integrated plan covering business and IT resources • Activities and interdependencies between projects	• *SD App D Design and planning documents and their contents*	
PO10.8 Project resources	• Responsibilities, relationships, authorities, and performance criteria of project team • Planning procurement of resources	• *ST 3.2.11 Proactively manage resources across service transitions*	
PO10.9 Project risk management	• Systematic process for planning, identifying, analysing, responding to, monitoring and controlling risks		
PO10.10 Project quality plan	• Defined and agreed-upon quality management plan and QMS		
PO10.11 Project change control	• Change control system for each project (cost, schedule, scope, quality)	• **ST 3.2.10 Anticipate and manage course corrections**	
PO10.12 Project planning of assurance methods	• Assurance tasks required to support accreditation		

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives: Plan & Organize (PO)



PO10 Manage Projects *(cont.)*			
CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
PO10.13 Project performance measurement, reporting and monitoring	• Measuring project performance against key criteria • Assessing deviations, recommending and implementing remedial actions		
PO10.14 Project closure	• Project stakeholders' review of achievement of results and benefits • Communicating outstanding actions and documenting lessons learned		

Summary, Conclusions & Questions

Thank you all for your courteous time and attention today:

- Please Note: We' ll be open to and available for discussing any & all areas addressed during this presentation.

Respectfully yours,

Pw Carey
Consultant CISA-CISSP
Compliance Partners, LLC
1250 Grove Avenue, Suite 200
Barrington, IL 60010
pwc.pwcarey@gmail.com/
pwcarey@complysys.com
650-278-3731 or 224-633-1378
Fax: 847-381-2067

Mapping ITIL V3 and ISO/IEC 27002 With CobiT 4.1 Control Objectives References

1. *Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit ® A Management Briefing From ITGI and OGC*

Copies of ISO/IEC 27002:2005 and all ISO standards can be purchased from the American National Standards Institute (ANSI) at http://webstore.ansi.org, phone: +1.212.642.4980; BSI in the UK (www.bsi-global.com/shop.html); and ISO (www.iso.org/iso/store.htm).