Cross reference COBIT – ISM

Auteur: J. van Bon (BHVB)

Datum: 9 maart 2009

Cross reference COBIT – ISM

Inleiding

Integrated Service Management™ (ISM) is een kwaliteitsmanagementsysteem voor IT-serviceorganisaties, waarmee de werkwijze van een IT-organisatie wordt ondersteund. Het ISM-framework bestaat uit een procesmodel, een integratie met een set van tools, een serie templates, een organisatiebeschrijving, een standaard definitiestelsel, en een implementatie-aanpak.

COBIT™ is een framework voor IT-managementorganisaties, waarin een uitgebreide serie 'control objectives' is gedocumenteerd" praktische zaken die moeten zijn geregeld wil een organisatie 'in control' zijn van haar IT. COBIT is van nature een audit-systeem, en wordt dan ook breed ingezet om te toetsen in hoeverre een IT-organisatie de vereiste beheersing heeft over deze IT.

Op verzoek van Infodis is een cross-reference gemaakt tussen beide frameworks. Doelstelling daarbij was het verkrijgen van een antwoord op de vraag in hoeverre het hanteren van ISM voorziet in een dekking van COBIT. Ten aanzien van ISM is deze cross-reference toegepast op het ISM-procesmodel, aangezien dat de enige 'harde' component is die door ISM wordt bepaald. Een groot deel van de control objectives van COBIT heeft te maken met de mate waarin een organisatie iets in praktijk heeft gebracht. In de cross-reference wordt dus beschreven welke dekking ISM heeft, mits de organisatie die van ISM gebruik maakt ook daadwerkelijk de ISM-werkwijze in de praktijk brengt.

Maturity

Infodis is geaudit op basis van het door Philips gehanteerde BEST-systeem. In BEST zijn de COBIT control objectives vertaald naar concrete prestatiekarakteristieken, die vervolgens zijn toegekend aan een niveau van het COBIT maturitysysteem. Dit maturitysysteem brengt een fasering aan ten aanzien van de mate waarin een organisatie een zekere control objective in de praktijk heeft gebracht. Het systeem onderscheidt 6 niveaus (0-5) en differentieert op ieder niveau naar een zestal aspecten:

- Awareness and Communication
- Policies, Standards and Procedures
- Tools and Automation
- Skills and Expertise
- Responsibility and Accountability
- Goal Setting and Measurement

ISM is een discreet model en kent dus geen maturitylevels, en we kunnen dus uitsluitend vaststellen in hoeverre ISM voorziet in elementen van elk van deze aspecten. Daarnaast kunnen we wel aanduiden op welk maturitylevel van het gehanteerde maturitysysteem dat zich bevindt, maar dat is weer een interpretatie, net zoals het maturitysysteem van BEST een COBIT-interpretatie van Philips is.

Het betreffende maturitysysteem is van het type 'continuous', hetgeen zoveel wil zeggen als dat alle activiteiten op ieder maturitylevel voorkomen, maar steeds in kwaliteit van uitvoering verschillen, oplopend van "not existent" tot "optimized".

De dekking van het BEST-maturitysysteem door ISM is op hoofdlijnen als volgt:

- **Awareness and Communication** – het toepassen van ISM betekent een **dekking op levels 4 en 5** van het maturitysysteem
- **Policies, Standards and Procedures** – het toepassen van ISM leidt tot een **volledige dekking van levels 4 en 5** van het maturitysysteem
- **Tools and Automation** – toepassen van ISM leidt tot een **volledige dekking op level 4**, en een organisatieafhankelijke invulling van aspecten op **level 5**
- **Skills and Expertise** – ISM voorziet niet in eisen en prestaties t.a.v. "skills and expertise". Dit aspect is dus **out-of-scope** en geheel organisatieafhankelijk
- **Responsibility and Accountability** – het toepassen van ISM leidt tot een **dekking op level 3**, en een organisatieafhankelijke invulling van levels 4 en 5
- **Goal Setting and Measurement** – toepassen van ISM leidt tot een dekking van levels 4 en 5 die echter **sterk afhankelijk van de invulling in de organisatie** is

Afgezien van het aspect "skills and expertise" bereikt een organisatie met het toepassen van ISM dus in hoofdzaak minimaal level 3 en veelal levels 4 of 5. Daarbij moet wel worden bedacht dat dit alleen geldt voor de tactische en operationele onderwerpen die door ISM worden gedekt. Weliswaar is dat het leeuwendeel, maar uit de cross-reference blijkt dat een deel van de strategische objectices uit COBIT out-of-scope zijn voor ISM.

Om vast te stellen of een organisatie de in ISM gespecificeerde werkwijze daadwerkelijk in praktijk brengt zal de organisatie vanzelfsprekend bewijsstukken moeten kunnen overleggen. Hieronder vallen bijvoorbeeld de in ISM genoemde documenten, zoals een SLA, een Service Catalog, een RFC-formulier, et cetera. In die documenten dient dan de concrete dekking van de in ISM genoemde aspecten te zijn toegepast.

High level cross-reference

Bij de high-level cross-reference is aangegeven hoe de dekking van ISM is t.a.v. de high-level control objectives. Uit de navolgende figuur volgt dat ISM een lichte dekking heeft in het PO-domein, een sterke dekking in het AI-domein, een volledige dekking in het DS-domein, en een bijna volledige dekking in het ME-domein.

De dekking door ISM is in de cross-reference gecategoriseerd volgens een systeem van 4 niveaus:

1. **Completely covered** – ISM voorziet volledig en expliciet in de betreffende karakeristiek
2. **Largely covered** – ISM voorziet in de karakteristiek, maar invullingen kunnen in detail afhankelijk zijn van wat de organisatie er in de praktijk van maakt
3. **Supported** – ISM zelf voorziet niet in de karakteristiek, maar biedt wel structuren die als ondersteuning daarvoor kunnen dienen
4. **Not explicitly covered** – karakteristieken die buiten de scope van ISM vallen

High level dekking van COBIT door ISM

Domain	High level objective in COBIT 4.1	High-level coverage in ISM: 1-2-3-4			
		LEGEND			
		COMPLETELY COVERED, explicit	**LARGELY COVERED**, sometimes more implicit than explicit	**SUPPORTED**, but often a responsibility of the local organization	**NOT EXPLICITLY COVERED**
Plan and Organise	**PO1 Define a strategic IT plan**				■
	PO2 Define the information architecture			■	■
	PO3 Determine technological direction				■
	PO4 Define the IT processes, organisation and relationships		■	■	■
	PO5 Manage the IT investment			■	■
	PO6 Communicate management aims and direction			■	■
	PO7 Manage IT human resources	■	■	■	
	PO8 Manage quality	■	■	■	
	PO9 Assess and manage IT risks	■	■		
	PO10 Manage projects			■	
Acquire and Implement	**AI1 Identify automated solutions**		■	■	■
	AI2 Acquire and maintain application software	■	■	■	
	AI3 Acquire and maintain technology infrastructure	■	■	■	
	AI4 Enable operation and use	■			
	AI5 Procure IT resources		■	■	
	AI6 Manage changes	■			
	AI7 Install and accredit solutions and changes	■			
Deliver and Support	**DS1 Define and manage service levels**	■			
	DS2 Manage third-party services		■		
	DS3 Manage performance and capacity	■	■		
	DS4 Ensure continuous service	■	■		
	DS5 Ensure systems security	■	■		
	DS6 Identify and allocate costs		■		

	DS7 Educate and train users		🟩		
	DS8 Manage service desk and incidents	🟩	🟩		
	DS9 Manage the configuration	🟩			
	DS10 Manage problems	🟩			
	DS11 Manage data		🟩		
	DS12 Manage the physical environment		🟩		
	DS13 Manage operations	🟩	🟩		
Monitor and Evaluate	**ME1 Monitor and evaluate IT performance**	🟩	🟩		
	ME2 Monitor and evaluate internal control	🟩	🟩		▨
	ME3 Ensure compliance with external requirements		🟩		▨
	ME4 Provide IT governance		🟩	🟨	▨

Detaillering van de cross-reference

Op de volgende pagina's is de cross-reference in detail uitgewerkt. Van elk COBIT-domein zijn de *high level objectives* benoemd, en daarbij zijn steeds de afzondelijke *detailed objectives* opgevoerd.

Per *detailed objective* is vervolgens aangegeven of, en in welke mate ISM in de betreffende karakteristiek voorziet. In de analyse is gebruik gemaakt van de meest recente versie van COBIT: versie 4.1. NB: bij de BEST-assessment is gebruik gemaakt van versie 4.0.

De dekking door ISM is opnieuw gecategoriseerd volgens het systeem van 4 niveaus:

1. **Completely covered** – ISM voorziet volledig en expliciet in de betreffende karakeristiek
2. **Largely covered** – ISM voorziet in de karakteristiek, maar invullingen kunnen in detail afhankelijk zijn van wat de organisatie er in de praktijk van maakt
3. **Supported** – ISM zelf voorziet nioet in de karakteristiek, maar biedt wel structuren die als ondersteuning daarvoor kunnen dienen
4. **Not explicitly covered** – karakteristieken die buiten de scope van ISM vallen

Voor elke *detailed control objective* die enigermate door ISM is gedekt is vervolgens een toelichting verstrekt. In de daaropvolgende kolom is exact aangegeven welke ISM-component die dekking concreet maakt. Als laatste is een kolom toegevoegd waarin is aangegeven of de objective wel binnen het assessment-pofiel van BEST valt en dus voor die assessment relevant is.

Detailed cross-reference

Domain	**High level objective in COBIT 4.1**		**Detailed objective / activity in COBIT4.1** LEGEND **COMPLETELY COVERED**, explicit **LARGELY COVERED**, sometimes more implicit than explicit **SUPPORTED**, but often a responsibility of the local organization **NOT EXPLICITLY COVERED**	**Coverage** 1=completely 2=largely 3=supported 4=not explicitly	**Details on coverage in ISM**	references to ISM sections	Selected for assess-ment? Yes/no
Plan and Organise	**PO1 Define a strategic IT plan**	**PO1.1**	**PO1.1 IT Value Management** Work with the business to ensure that the enterprise portfolio of IT-enabled investments contains programmes that have solid business cases. Recognise that there are mandatory, sustaining and discretionary investments that differ in complexity and degree of freedom in allocating funds. IT processes should provide effective and efficient delivery of the IT components of programmes and early warning of any deviations from plan, including cost, schedule or functionality, that might impact the expected outcomes of the programmes. IT services should be executed against equitable and enforceable service level agreements (SLAs). Accountability for achieving the benefits and controlling the costs should be clearly assigned and monitored. Establish fair, transparent, repeatable and comparable evaluation of business cases, including financial worth, the risk of not delivering a capability and the risk of not realising the expected benefits.	4	Not explicitly covered.		yes
		PO1.2	**PO1.2 Business-IT Alignment** Establish processes of bi-directional education and reciprocal involvement in strategic planning to achieve business and IT alignment and integration. Mediate between business and IT imperatives so priorities can be mutually agreed.	4	Not explicitly covered.		yes
		PO1.3	**PO1.3 Assessment of Current Capability and Performance** Assess the current capability and performance of solution and service delivery to establish a baseline against which future requirements can be compared. Define performance in terms of IT's contribution to business objectives, functionality, stability, complexity, costs, strengths and weaknesses.	4	Not explicitly covered, although this can be supported by the Service Catalog, the SLAs, and all reporting in SLM.		yes
		PO1.4	**PO1.4 IT Strategic Plan** Create a strategic plan that defines, in co-operation with relevant stakeholders, how IT goals will contribute to the enterprise's strategic objectives and related costs and risks. It should include how IT will support IT-enabled investment programmes, IT services and IT assets. IT should define how the objectives will be met, the measurements to be used and the procedures to obtain formal sign-off from the stakeholders. The IT strategic plan should cover investment/operational budget, funding sources, sourcing	4	Not explicitly covered.		yes

			strategy, acquisition strategy, and legal and regulatory requirements. The strategic plan should be sufficiently detailed to allow for the definition of tactical IT plans.				
		PO1.5	**PO1.5 IT Tactical Plans** Create a portfolio of tactical IT plans that are derived from the IT strategic plan. The tactical plans should address IT-enabled programme investments, IT services and IT assets. The tactical plans should describe required IT initiatives, resource requirements, and how the use of resources and achievement of benefits will be monitored and managed. The tactical plans should be sufficiently detailed to allow the definition of project plans. Actively manage the set of tactical IT plans and initiatives through analysis of project and service portfolios.	4	Not explicitly covered.		yes
		PO1.6	**PO1.6 IT Portfolio Management** Actively manage with the business the portfolio of IT-enabled investment programmes required to achieve specific strategic business objectives by identifying, defining, evaluating, prioritising, selecting, initiating, managing and controlling programmes. This should include clarifying desired business outcomes, ensuring that programme objectives support achievement of the outcomes, understanding the full scope of effort required to achieve the outcomes, assigning clear accountability with supporting measures, defining projects within the programme, allocating resources and funding, delegating authority, and commissioning required projects at programme launch.	4	Not explicitly covered, but this can be supported by the CHM process if the projects are registered as RFCs.		yes
	PO2 Define the information architecture	**PO2.1**	**PO2.1 Enterprise Information Architecture Model** Establish and maintain an enterprise information model to enable applications development and decision-supporting activities, consistent with IT plans as described in PO1. The model should facilitate the optimal creation, use and sharing of information by the business in a way that maintains integrity and is flexible, functional, cost-effective, timely, secure and resilient to failure.	4	Not explicitly covered.		no
		PO2.2	**PO2.2 Enterprise Data Dictionary and Data Syntax Rules** Maintain an enterprise data dictionary that incorporates the organisation's data syntax rules. This dictionary should enable the sharing of data elements amongst applications and systems, promote a common understanding of data amongst IT and business users, and prevent incompatible data elements from being created.	4	Not explicitly covered.		no
		PO2.3	**PO2.3 Data Classification Scheme** Establish a classification scheme that applies throughout the enterprise, based on the criticality and sensitivity (e.g., public, confidential, top secret) of enterprise data. This scheme should include details about data ownership; definition of appropriate security levels and protection controls; and a brief description of data retention and	3	Infrastructure specific. Can be applied in procedures and in templates, but not covered in the generic process model.		no

			destruction requirements, criticality and sensitivity. It should be used as the basis for applying controls such as access controls, archiving or encryption.				
		PO2.4	**PO2.4 Integrity Management** Define and implement procedures to ensure the integrity and consistency of all data stored in electronic form, such as databases, data warehouses and data archives.	3	Infrastructure specific. Can be applied in procedures and in templates, but not covered in the generic process model.		no
	PO3 Determine technological direction	**PO3.1**	**PO3.1 Technological Direction Planning** Analyse existing and emerging technologies, and plan which technological direction is appropriate to realise the IT strategy and the business systems architecture. Also identify in the plan which technologies have the potential to create business opportunities. The plan should address systems architecture, technological direction, migration strategies and contingency aspects of infrastructure components.	4	Not explicitly covered.		yes
		PO3.2	**PO3.2 Technology Infrastructure Plan** Create and maintain a technology infrastructure plan that is in accordance with the IT strategic and tactical plans. The plan should be based on the technological direction and include contingency arrangements and direction for acquisition of technology resources. It should consider changes in the competitive environment, economies of scale for information systems staffing and investments, and improved interoperability of platforms and applications.	4	Not explicitly covered.		yes
		PO3.3	**PO3.3 Monitor Future Trends and Regulations** Establish a process to monitor the business sector, industry, technology, infrastructure, legal and regulatory environment trends. Incorporate the consequences of these trends into the development of the IT technology infrastructure plan.	4	Not explicitly covered.		yes
		PO3.4	**PO3.4 Technology Standards** To provide consistent, effective and secure technological solutions enterprisewide, establish a technology forum to provide technology guidelines, advice on infrastructure products and guidance on the selection of technology, and measure compliance with these standards and guidelines. This forum should direct technology standards and practices based on their business relevance, risks and compliance with external requirements.	4	Not explicitly covered.		yes
	PO4 Define the IT processes, organisation and relationships	**PO4.1**	**PO4.1 IT Process Framework** Define an IT process framework to execute the IT strategic plan. This framework should include an IT process structure and relationships (e.g., to manage process gaps and overlaps), ownership, maturity, performance measurement, improvement, compliance, quality targets and plans to achieve them. It should provide integration amongst the processes that are specific to IT, enterprise portfolio management, business processes and business change processes. The IT process framework should be integrated into a quality management system (QMS) and the internal control framework.	2	The ISM Process Model is the 'process framework'. The ISM Process Model contains structure and relationships between processes. The RACI structure in the publishing tool can contain the role 'process owner', if the organization has indeed created this role. No differentiation in terms of maturity, but organizations can in fact determine the level of detail of process specs they want to use. The activity descriptions contain performance requirements and targets. Implementation plans are covered by the ISM Project Approach.	ISM	yes

					The ISM Processs Model is an integrated model, with a full input/output validation. The ISM Pocess Model is implemented in a Quality Management System, i.e. the publication tool, which is an element of the organizations' management framework. The ISM Process Model is fully integrated wit a workflow support system.		
		PO4.2	**PO4.2 IT Strategy Committee** Establish an IT strategy committee at the board level. This committee should ensure that IT governance, as part of enterprise governance, is adequately addressed; advise on strategic direction; and review major investments on behalf of the full board.	3	Can be covered in Process Publishing Tool, depending upon local organization.		yes
		PO4.3	**PO4.3 IT Steering Committee** Establish an IT steering committee (or equivalent) composed of executive, business and IT management to: • Determine prioritisation of IT-enabled investment programmes in line with the enterprise's business strategy and priorities • Track status of projects and resolve resource conflict • Monitor service levels and service improvements	3	Can be covered in Process Publishing Tool, depending upon local organization.		yes
		PO4.4	**PO4.4 Organisational Placement of the IT Function** Place the IT function in the overall organisational structure with a business model contingent on the importance of IT within the enterprise, specifically its criticality to business strategy and the level of operational dependence on IT. The reporting line of the CIO should be commensurate with the importance of IT within the enterprise.	3	Can be covered in Process Publishing Tool, depending upon local organization.		yes
		PO4.5	**PO4.5 IT Organisational Structure** Establish an internal and external IT organisational structure that reflects business needs. In addition, put a process in place for periodically reviewing the IT organisational structure to adjust staffing requirements and sourcing strategies to meet expected business objectives and changing circumstances.	3	Can be covered in Process Publishing Tool, depending upon local organization.		yes
		PO4.6	**PO4.6 Establishment of Roles and Responsibilities** Establish and communicate roles and responsibilities for IT personnel and end users that delineate between IT personnel and end-user authority, responsibilities and accountability for meeting the organisation's needs.	2	The Process Publishing Tool integrates all roles and responsibilities with Activities through a RACI framework.	ISM	yes
		PO4.7	**PO4.7 Responsibility for IT Quality Assurance** Assign responsibility for the performance of the quality assurance (QA) function and provide the QA group with appropriate QA systems, controls and communications expertise. Ensure that the organisational placement and the responsibilities and size of the QA group satisfy the requirements of the organisation.	3	Can be covered in Process Publishing Tool, depending upon local organization.		yes

		PO4.8	**PO4.8 Responsibility for Risk, Security and Compliance** Embed ownership and responsibility for IT-related risks within the business at an appropriate senior level. Define and assign roles critical for managing IT risks, including the specific responsibility for information security, physical security and compliance. Establish risk and security management responsibility at the enterprise level to deal with organisationwide issues. Additional security management responsibilities may need to be assigned at a system-specific level to deal with related security issues. Obtain direction from senior management on the appetite for IT risk and approval of any residual IT risks.	3	Can be covered in Process Publishing Tool, depending upon local organization.		yes
		PO4.9	**PO4.9 Data and System Ownership** Provide the business with procedures and tools, enabling it to address its responsibilities for ownership of data and information systems. Owners should make decisions about classifying information and systems and protecting them in line with this classification.	3	Can be covered in Process Publishing Tool, depending upon local organization.		yes
		PO4.10	**PO4.10 Supervision** Implement adequate supervisory practices in the IT function to ensure that roles and responsibilities are properly exercised, to assess whether all personnel have sufficient authority and resources to execute their roles and responsibilities, and to generally review KPIs.	3	Can be covered in Process Publishing Tool, depending upon local organization.		yes
		PO4.11	**PO4.11 Segregation of Duties** Implement a division of roles and responsibilities that reduces the possibility for a single individual to compromise a critical process. Make sure that personnel are performing only authorised duties relevant to their respective jobs and positions.	3	Can be covered in Process Publishing Tool, depending upon local organization.		yes
		PO4.12	**PO4.12 IT Staffing** Evaluate staffing requirements on a regular basis or upon major changes to the business, operational or IT environments to ensure that the IT function has sufficient resources to adequately and appropriately support the business goals and objectives.	4	Not explicitly covered.		yes
		PO4.13	**PO4.13 Key IT Personnel** Define and identify key IT personnel (e.g., replacements/backup personnel), and minimise reliance on a single individual performing a critical job function.	3	Can be covered in Process Publishing Tool, depending upon local organization.		yes
		PO4.14	**PO4.14 Contracted Staff Policies and Procedures** Ensure that consultants and contract personnel who support the IT function know and comply with the organisation's policies for the protection of the organisation's information assets such that they meet agreed-upon contractual requirements.	4	Not explicitly covered.		yes
		PO4.15	**PO4.15 Relationships** Establish and maintain an optimal co-ordination, communication and liaison structure between the IT function and various other interests inside and outside the IT function, such as the board, executives, business units, individual users, suppliers, security officers, risk managers, the corporate compliance group, outsourcers and offsite management.	3	Can be covered in Process Publishing Tool, depending upon local organization.		yes

	PO5 Manage the IT investment	**PO5.1**	**PO5.1 Financial Management Framework** Establish and maintain a financial framework to manage the investment and cost of IT assets and services through portfolios of IT-enabled investments, business cases and IT budgets.	3	Can be covered by a function, using the single processes in the ISM Process Model. Can be covered in Process Publishing Tool.		no
		PO5.2	**PO5.2 Prioritisation Within IT Budget** Implement a decision-making process to prioritise the allocation of IT resources for operations, projects and maintenance to maximise IT's contribution to optimising the return on the enterprise's portfolio of IT-enabled investment programmes and other IT services and assets.	3	Covered by the CHM process in the ISM Process Model, or in a specific procedure following that process.		no
		PO5.3	**PO5.3 IT Budgeting** Establish and implement practices to prepare a budget reflecting the priorities established by the enterprise's portfolio of IT-enabled investment programmes, and including the ongoing costs of operating and maintaining the current infrastructure. The practices should support development of an overall IT budget as well as development of budgets for individual programmes, with specific emphasis on the IT components of those programmes. The practices should allow for ongoing review, refinement and approval of the overall budget and the budgets for individual programmes.	3	Can be covered by a function, using the single processes in the ISM Process Model. Can be covered in Process Publishing Tool.		no
		PO5.4	**PO5.4 Cost Management** Implement a cost management process comparing actual costs to budgets. Costs should be monitored and reported. Where there are deviations, these should be identified in a timely manner and the impact of those deviations on programmes should be assessed. Together with the business sponsor of those programmes, appropriate remedial action should be taken and, if necessary, the programme business case should be updated.	3	Can be covered by a function, using the single processes in the ISM Process Model. Can be covered in Process Publishing Tool.		no
		PO5.5	**PO5.5 Benefit Management** Implement a process to monitor the benefits from providing and maintaining appropriate IT capabilities. IT's contribution to the business, either as a component of IT-enabled investment programmes or as part of regular operational support, should be identified and documented in a business case, agreed to, monitored and reported. Reports should be reviewed and, where there are opportunities to improve IT's contribution, appropriate actions should be defined and taken. Where changes in IT's contribution impact the programme, or where changes to other related projects impact the programme, the programme business case should be updated.	4	Not explicitly covered.		no
	PO6 Communicate management aims and direction	**PO6.1**	**PO6.1 IT Policy and Control Environment** Define the elements of a control environment for IT, aligned with the enterprise's management philosophy and operating style. These elements should include expectations/requirements regarding delivery of value from IT investments, appetite for risk, integrity, ethical values, staff competence, accountability and responsibility. The control environment should be based on a culture that supports value delivery whilst managing significant risks, encourages cross-divisional co-operation and teamwork, promotes compliance and continuous process improvement, and handles process deviations (including failure) well.	4	Not explicitly covered.		no

		PO6.2	**PO6.2 Enterprise IT Risk and Control Framework** Develop and maintain a framework that defines the enterprise's overall approach to IT risk and control and that aligns with the IT policy and control environment and the enterprise risk and control framework.	3	Supported by the QM process in the ISM Process Model. QM identifies risks, and controls these by selecting and implementing appropriate measures.		no
		PO6.3	**PO6.3 IT Policies Management** Develop and maintain a set of policies to support IT strategy. These policies should include policy intent; roles and responsibilities; exception process; compliance approach; and references to procedures, standards and guidelines. Their relevance should be confirmed and approved regularly.	3	Supported by the ISM Process Model, and the set of procedures derived from that, as expressed in the Process Publication Tool.		no
		PO6.4	**PO6.4 Policy, Standard and Procedures Rollout** Roll out and enforce IT policies to all relevant staff, so they are built into and are an integral part of enterprise operations.	3	Supported by the ISM Process Model, and the set of procedures derived from that, as expressed in the Process Publication Tool.		no
		PO6.5	**PO6.5 Communication of IT Objectives and Direction** Communicate awareness and understanding of business and IT objectives and direction to appropriate stakeholders and users throughout the enterprise.	4	Not explicitly covered.		no
	PO7 Manage IT human resources	**PO7.1**	**PO7.1 Personnel Recruitment and Retention** Maintain IT personnel recruitment processes in line with the overall organisation's personnel policies and procedures (e.g., hiring, positive work environment, orienting). Implement processes to ensure that the organisation has an appropriately deployed IT workforce with the skills necessary to achieve organisational goals.	2	Can be covered by applying CHM to personnel. Human resources would be required to be subject to the management system, and therefore also subject to the COM process.	CHM, COM	no
		PO7.2	**PO7.2 Personnel Competencies** Regularly verify that personnel have the competencies to fulfil their roles on the basis of their education, training and/or experience. Define core IT competency requirements and verify that they are being maintained, using qualification and certification programmes where appropriate.	2	Can be covered by means of COM. Human resources would be required to be subject to the management system, and their requirements in terms of skills would have to be registered as attributes of the CI "Personnel". All requires types of "Personnel" would have to be registered as CI types.	COM	no
		PO7.3	**PO7.3 Staffing of Roles** Define, monitor and supervise roles, responsibilities and compensation frameworks for personnel, including the requirement to adhere to management policies and procedures, the code of ethics, and professional practices. The level of supervision should be in line with the sensitivity of the position and extent of responsibilities assigned.	4	Not explicitly covered.		no
		PO7.4	**PO7.4 Personnel Training** Provide IT employees with appropriate orientation when hired and ongoing training to maintain their knowledge, skills, abilities, internal controls and security awareness at the level required to achieve organisational goals.	2	Can be covered by a Standard Change, for hiring new staff. If maintenance of their knowledge should be covered by the management system, the individual personnel "CIs" should be audited in the COM process against the required attributes of the CI type. Maintenance of competencies is covered in standard CHM process.	CHM4, CHM6, COM	no
		PO7.5	**PO7.5 Dependence Upon Individuals** Minimise the exposure to critical dependency on key individuals through knowledge capture (documentation), knowledge sharing, succession planning and staff backup.	3	The system can support the recognition of key individuals by means of reporting from the Process Publishing Tool.		no

		PO7.6	**PO7.6 Personnel Clearance Procedures** Include background checks in the IT recruitment process. The extent and frequency of periodic reviews of these checks should depend on the sensitivity and/or criticality of the function and should be applied for employees, contractors and vendors.	3	Can be covered in a Standard Change and in the configuration audits of PO7.4		no
		PO7.7	**PO7.7 Employee Job Performance Evaluation** Require a timely evaluation to be performed on a regular basis against individual objectives derived from the organisation's goals, established standards and specific job responsibilities. Employees should receive coaching on performance and conduct whenever appropriate.	4	Not explicitly covered.		no
		PO7.8	**PO7.8 Job Change and Termination** Take expedient actions regarding job changes, especially job terminations. Knowledge transfer should be arranged, responsibilities reassigned and access rights removed such that risks are minimised and continuity of the function is guaranteed.	2	Can be covered by applying the CHM process in the ISM Process Model. Human resources would be required to be subject to the management system, and therefore also subject to the COM process.	CHM, COM	no
	PO8 Manage quality	**PO8.1**	**PO8.1 Quality Management System** Establish and maintain a QMS that provides a standard, formal and continuous approach regarding quality management that is aligned with business requirements. The QMS should identify quality requirements and criteria; key IT processes and their sequence and interaction; and the policies, criteria and methods for defining, detecting, correcting and preventing non-conformity. The QMS should define the organisational structure for quality management, covering the roles, tasks and responsibilities. All key areas should develop their quality plans in line with criteria and policies and record quality data. Monitor and measure the effectiveness and acceptance of the QMS, and improve it when needed	1	The ISM proces Model is described in a QMS - the Process Publishing Tool. Alignment with business is done through Service Level Management. Quality requirements are covered in the SLA. Key IT processes and their sequence and interaction are covered in the ISM Process Model, including all Control processes. The organization structure is covered in the Publishing tool, including all RACI, roles, tasks, responsibilities. Quality plans can be set up by any team, following their specific tasks, using the processes. All processes are controlled and monitored. All teams can improve whenever required. The Quality Management proces covers the structural approach towards risk prevention, i.e. improvement.	ISM	yes
		PO8.2	**PO8.2 IT Standards and Quality Practices** Identify and maintain standards, procedures and practices for key IT processes to guide the organisation in meeting the intent of the QMS. Use industry good practices for reference when improving and tailoring the organisation's quality practices.	1	Can be achieved by using the Procedure templates based on the ISM Process Model. ISM aligns to industry best practices.	ISM	yes
		PO8.3	**PO8.3 Development and Acquisition Standards** Adopt and maintain standards for all development and acquisition that follow the life cycle of the ultimate deliverable, and include sign-off at key milestones based on agreed-upon sign-off criteria. Consider software coding standards; naming conventions; file formats; schema and data dictionary design standards; user interface standards; interoperability; system performance efficiency; scalability; standards for development and testing; validation against requirements; test plans; and unit, regression and integration testing.	2	Can be covered in the CHM process. Technical details can be organization-specific.	CHM	yes

		PO8.4	**PO8.4 Customer Focus** Focus quality management on customers by determining their requirements and aligning them to the IT standards and practices. Define roles and responsibilities concerning conflict resolution between the user/customer and the IT organisation.	2	Covered by the aligned systems of FSM and ISM, where ISM uses structured customer requirements as input for its management domain, in SLM1. Roles and responsibilities are organization-specific, but they are supported by the ISM processes SLM (on tactical level concerning contract issues) and IM (on operational level concerning delivery issues).	SLM, IM	yes
		PO8.5	**PO8.5 Continuous Improvement** Maintain and regularly communicate an overall quality plan that promotes continuous improvement.	2	All risks are registered in the risk database in QM1. Reporting from the risk database provides all information about status of risks. All service improvement proposals that are discussed and agreed with the customer are registered in the SIP in SLM2.3.	QM1, SLM2.3	yes
		PO8.6	**PO8.6 Quality Measurement, Monitoring and Review** Define, plan and implement measurements to monitor continuing compliance to the QMS, as well as the value the QMS provides. Measurement, monitoring and recording of information should be used by the process owner to take appropriate corrective and preventive actions.	3	ISM determines all kinds of registrations to support the processes. Also, for each process, ISM has a Control Process, responsible for the correct and timely performance of process steps.		yes
	PO9 Assess and manage IT risks	**PO9.1**	**PO9.1 IT Risk Management Framework** Establish an IT risk management framework that is aligned to the organisation's (enterprise's) risk management framework.	1	The Quality Management process is exactly that: Risk Management. It collects information on risks from various sources, determines impact ad priorities, selects countermeasures and sees that these are implemented to take away/mitigate the risk. Quality Management can be used by any function the organization had set up for any specific aspect of service quality.	QM	yes
		PO9.2	**PO9.2 Establishment of Risk Context** Establish the context in which the risk assessment framework is applied to ensure appropriate outcomes. This should include determining the internal and external context of each risk assessment, the goal of the assessment, and the criteria against which risks are evaluated.	1	The context of ISM is the quality of the agreed services. The QM (Risk) process is governed from any possible context that relates to service quality.	QM	yes
		PO9.3	**PO9.3 Event Identification** Identify events (an important realistic threat that exploits a significant applicable vulnerability) with a potential negative impact on the goals or operations of the enterprise, including business, regulatory, legal, technology, trading partner, human resources and operational aspects. Determine the nature of the impact and maintain this information. Record and maintain relevant risks in a risk registry.	1	Events are identified anywhere in the organization, in step 1 of the QM process. They are then qualified, recorded, and maintained in a risk database.	QM1	yes
		PO9.4	**PO9.4 Risk Assessment** Assess on a recurrent basis the likelihood and impact of all identified risks, using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk should be determined individually, by category and on a portfolio basis.	2	QM Process Control sees to a continuous monitoring of the QM process, including evaluation of priorities. Registration of risk characteristics is done in step QM1, and can be detailed to any required level a customer organization requires. This should be covered in organization-specific work-instructions.	QM1	yes

		PO9.5	**PO9.5 Risk Response** Develop and maintain a risk response process designed to ensure that cost-effective controls mitigate exposure to risks on a continuing basis. The risk response process should identify risk strategies such as avoidance, reduction, sharing or acceptance; determine associated responsibilities; and consider risk tolerance levels.	2	This again is standard procedure in ISM's QM process. Details are covered in organization-specific work-instructions.	QM	yes
		PO9.6	**PO9.6 Maintenance and Monitoring of a Risk Action Plan** Prioritise and plan the control activities at all levels to implement the risk responses identified as necessary, including identification of costs, benefits and responsibility for execution. Obtain approval for recommended actions and acceptance of any residual risks, and ensure that committed actions are owned by the affected process owner(s). Monitor execution of the plans, and report on any deviations to senior management.	1	This is standard procedure in the QM and CHM process. The CHM process is triggered by the QM process to take action against identified risks. The alternative outcome of the QM process is a request to adapt the SLA, which can be part of the Service Improvement program (SIP) in SLM2.	QM, CHM, SLM2	yes
	PO10 Manage projects	**PO10.1**	**PO10.1 Programme Management Framework** Maintain the programme of projects, related to the portfolio of IT-enabled investment programmes, by identifying, defining, evaluating, prioritising, selecting, initiating, managing and controlling projects. Ensure that the projects support the programme's objectives. Co-ordinate the activities and interdependencies of multiple projects, manage the contribution of all the projects within the programme to expected outcomes, and resolve resource requirements and conflicts.	3	Project management, program management, and portfolio management are out-of-scope for ISM since they are in the customer domain. Portfolios of programmes with specific projects always result in either: 1) service delivery proposals in the SLM process 2) RFCs triggering the CHM process 3) service requests triggering the OM process Programme management is only supported at interface level with the customer organization. Project management can be used as a work-instruction level choice for each activity or step in any ISM process. It's up to the organization to decide whether they wish to spend heavy resources on a specific step. Therefore these aspects of project management are subject to organization-specific choices. Projects can also result in triggers to standard ISM processes, like the CHM process: a project can be realized through an RFC. In cases like that, the standard ISM process definition applies and project management represents the process customer. Methods for project management are also at the work-instruction level of ISM activities, and therefor organization-specific. Project management in a pre-effective phase is out-of-scope of ISM, since it is in fact decision making on the specifications of triggers like RFCs.		no

		PO10.2	**PO10.2 Project Management Framework** Establish and maintain a project management framework that defines the scope and boundaries of managing projects, as well as the method to be adopted and applied to each project undertaken. The framework and supporting method should be integrated with the programme management processes.	3	See comments at PO 10.1		no
		PO10.3	**PO10.3 Project Management Approach** Establish a project management approach commensurate with the size, complexity and regulatory requirements of each project. The project governance structure can include the roles, responsibilities and accountabilities of the programme sponsor, project sponsors, steering committee, project office and project manager, and the mechanisms through which they can meet those responsibilities (such as reporting and stage reviews). Make sure all IT projects have sponsors with sufficient authority to own the execution of the project within the overall strategic programme.	3	See comments at PO 10.1 E.g. IT project sponsorship can be covered in the CHM process.		no
		PO10.4	**PO10.4 Stakeholder Commitment** Obtain commitment and participation from the affected stakeholders in the definition and execution of the project within the context of the overall IT-enabled investment programme.	3	See comments at PO 10.1 As soon as projects are getting effective, they result in a change or any other standard ISM process step, and IT project stakeholder commitment and participation is covered in the intake phase of the CHM process or the relevant step. E.g. participation is covered in the Change Advisory Board in the CHM process.		no
		PO10.5	**PO10.5 Project Scope Statement** Define and document the nature and scope of the project to confirm and develop amongst stakeholders a common understanding of project scope and how it relates to other projects within the overall IT-enabled investment programme. The definition should be formally approved by the programme and project sponsors before project initiation.	3	See comments at PO 10.1 Any specific requirement on project management is organization-specific.		no
		PO10.6	**PO10.6 Project Phase Initiation** Approve the initiation of each major project phase and communicate it to all stakeholders. Base the approval of the initial phase on programme governance decisions. Approval of subsequent phases should be based on review and acceptance of the deliverables of the previous phase, and approval of an updated business case at the next major review of the programme. In the event of overlapping project phases, an approval point should be established by programme and project sponsors to authorise project progression.	3	See comments at PO 10.1		no
		PO10.7	**PO10.7 Integrated Project Plan** Establish a formal, approved integrated project plan (covering business and information systems resources) to guide project execution and control throughout the life of the project. The activities and interdependencies of multiple projects within a programme should be understood and documented. The project plan should be maintained throughout the life of the project. The project plan, and changes to it, should be approved in line with the programme and project governance framework.	3	See comments at PO 10.1		no

		PO10.8	**PO10.8 Project Resources** Define the responsibilities, relationships, authorities and performance criteria of project team members, and specify the basis for acquiring and assigning competent staff members and/or contractors to the project. The procurement of products and services required for each project should be planned and managed to achieve project objectives using the organisation's procurement practices.	3	See comments at PO 10.1		no
		PO10.9	**PO10.9 Project Risk Management** Eliminate or minimise specific risks associated with individual projects through a systematic process of planning, identifying, analysing, responding to, monitoring and controlling the areas or events that have the potential to cause unwanted change. Risks faced by the project management process and the project deliverable should be established and centrally recorded.	3	See comments at PO 10.1 Can also be covered in QM process.		no
		PO10.10	**PO10.10 Project Quality Plan** Prepare a quality management plan that describes the project quality system and how it will be implemented. The plan should be formally reviewed and agreed to by all parties concerned and then incorporated into the integrated project plan.	3	See comments at PO 10.1		no
		PO10.11	**PO10.11 Project Change Control** Establish a change control system for each project, so all changes to the project baseline (e.g., cost, schedule, scope, quality) are appropriately reviewed, approved and incorporated into the integrated project plan in line with the programme and project governance framework.	3	See comments at PO 10.1 High-level projects can cover several changes, but these are then processed along standard CHM process. Projects can also be work-instructions in the CHM process, and then the comments of 10.5 apply.		no
		PO10.12	**PO10.12 Project Planning of Assurance Methods** Identify assurance tasks required to support the accreditation of new or modified systems during project planning, and include them in the integrated project plan. The tasks should provide assurance that internal controls and security features meet the defined requirements.	3	See comments at PO 10.1		no
		PO10.13	**PO10.13 Project Performance Measurement, Reporting and Monitoring** Measure project performance against key project performance scope, schedule, quality, cost and risk criteria. Identify any deviations from the plan. Assess the impact of deviations on the project and overall programme, and report results to key stakeholders. Recommend, implement and monitor remedial action, when required, in line with the programme and project governance framework.	3	See comments at PO 10.1		no
		PO10.14	**PO10.14 Project Closure** Require that, at the end of each project, the project stakeholders ascertain whether the project delivered the planned results and benefits. Identify and communicate any outstanding activities required to achieve the planned results of the project and the benefits of the programme, and identify and document lessons learned for use on future projects and programmes.	3	See comments at PO 10.1		no
Acquire and Implement	**AI1 Identify automated solutions**	**AI1.1**	**AI1.1 Definition and Maintenance of Business Functional and Technical Requirements** Identify, prioritise, specify and agree on business functional and technical requirements covering the full scope of all	2	Covered in SLM1 The level of detail is determined at work-instruction level, i.e. organization-specific.	SLM1	no

			initiatives required to achieve the expected outcomes of the IT-enabled investment programme.				
		AI1.2	**AI1.2 Risk Analysis Report** Identify, document and analyse risks associated with the business requirements and solution design as part of the organisation's process for the development of requirements.	4	Part of the Functional Management domain. Decision takening element, out-of-scope for ISM.		no
		AI1.3	**AI1.3 Feasibility Study and Formulation of Alternative Courses of Action** Develop a feasibility study that examines the possibility of implementing the requirements. Business management, supported by the IT function, should assess the feasibility and alternative courses of action and make a recommendation to the business sponsor.	4	Part of the Functional Management domain. Decision takening element, out-of-scope for ISM.		no
		AI1.4	**AI1.4 Requirements and Feasibility Decision and Approval** Verify that the process requires the business sponsor to approve and sign off on business functional and technical requirements and feasibility study reports at predetermined key stages. The business sponsor should make the final decision with respect to the choice of solution and acquisition approach.	3	This is largely at the work-instruction level of steps in SLM and CHM process.		no
	AI2 Acquire and maintain application software	**AI2.1**	**AI2.1 High-level Design** Translate business requirements into a high-level design specification for software acquisition, taking into account the organisation's technological direction and information architecture. Have the design specifications approved by management to ensure that the high-level design responds to the requirements. Reassess when significant technical or logical discrepancies occur during development or maintenance.	2	This can be covered in service specsheets (SLM) and in change specifications (CHM), at work-instruction level.	SLM1, CHM1, CHM2, CHM4	yes
		AI2.2	**AI2.2 Detailed Design** Prepare detailed design and technical software application requirements. Define the criteria for acceptance of the requirements. Have the requirements approved to ensure that they correspond to the high-level design. Perform reassessment when significant technical or logical discrepancies occur during development or maintenance.	2	This can be covered in service specsheets (SLM) and in change specifications (CHM), at work-instruction level.	SLM1, CHM1, CHM2, CHM4	yes
		AI2.3	**AI2.3 Application Control and Auditability** Implement business controls, where appropriate, into automated application controls such that processing is accurate, complete, timely, authorised and auditable.	3	Implementation-dependent: can be covered in service specsheets (SLM) and in change specifications (CHM), at work-instruction level.		yes
		AI2.4	**AI2.4 Application Security and Availability** Address application security and availability requirements in response to identified risks and in line with the organisation's data classification, information architecture, information security architecture and risk tolerance.	3	This can be covered in service specsheets (SLM) and in change specifications (CHM), at work-instruction level.		yes
		AI2.5	**AI2.5 Configuration and Implementation of Acquired Application Software** Configure and implement acquired application software to meet business objectives.	1	Fully covered in the CHM process.	CHM	yes
		AI2.6	**AI2.6 Major Upgrades to Existing Systems** In the event of major changes to existing systems that result in significant change in current designs and/or functionality, follow a similar development process as that used for the development of new systems.	1	Fully covered in the CHM process.	CHM	yes

		AI2.7	**AI2.7 Development of Application Software** Ensure that automated functionality is developed in accordance with design specifications, development and documentation standards, QA requirements, and approval standards. Ensure that all legal and contractual aspects are identified and addressed for application software developed by third parties.	1	Fully covered in the CHM process.	CHM	yes
		AI2.8	**AI2.8 Software Quality Assurance** Develop, resource and execute a software QA plan to obtain the quality specified in the requirements definition and the organisation’s quality policies and procedures.	3	This is subject to the standard CHM process, and can be covered at work-instruction level.	CHM	yes
		AI2.9	**AI2.9 Applications Requirements Management** Track the status of individual requirements (including all rejected requirements) during the design, development and implementation, and approve changes to requirements through an established change management process.	2	This is subject to the standard CHM process, and can be covered at work-instruction level.	CHM	yes
		AI2.10	**AI2.10 Application Software Maintenance** Develop a strategy and plan for the maintenance of software applications.	1	This is subject to the standard OM process, as a consequence of SLA obligations. Covered in the operations plan.	OM1	yes
	AI3 Acquire and maintain technology infrastructure	**AI3.1**	**AI3.1 Technological Infrastructure Acquisition Plan** Produce a plan for the acquisition, implementation and maintenance of the technological infrastructure that meets established business functional and technical requirements and is in accord with the organisation’s technology direction.	3	This is a task for organizational functions like capacity management, availability management, or continuity management. These functions all use the 6 ISM processes for the execution of their plans. Changes to the infrastructure are all run through the CHM process.		yes
		AI3.2	**AI3.2 Infrastructure Resource Protection and Availability** Implement internal control, security and auditability measures during configuration, integration and maintenance of hardware and infrastructural software to protect resources and ensure availability and integrity. Responsibilities for using sensitive infrastructure components should be clearly defined and understood by those who develop and integrate infrastructure components. Their use should be monitored and evaluated.	3	This is a task for organizational functions like security management, application management or Operations. These functions all use the 6 ISM processes for the execution of their plans. Changes to the infrastructure are all run through the CHM process. Monitoring of sensitive infrastructure components will be specified in the Operations plan and executed in the OM process.		yes
		AI3.3	**AI3.3 Infrastructure Maintenance** Develop a strategy and plan for infrastructure maintenance, and ensure that changes are controlled in line with the organisation’s change management procedure. Include periodic reviews against business needs, patch management, upgrade strategies, risks, vulnerabilities assessment and security requirements.	2	This is the result when using all 6 ISM processes. Maintenance plans will be a consequence of SLAs and registered in Operations plans or tactical function plans (e.g. Capacity plan, Security plan). CHM takes care of all changes. QM will cover all risks that are signalled by any of the organization's teams.	ISM	yes
		AI3.4	**AI3.4 Feasibility Test Environment** Establish development and test environments to support effective and efficient feasibility and integration testing of infrastructure components.	1	Fully covered in the CHM process.	CHM5	yes
	AI4 Enable operation and use	**AI4.1**	**AI4.1 Planning for Operational Solutions** Develop a plan to identify and document all technical, operational and usage aspects such that all those who will operate, use and maintain the automated solutions can exercise their responsibility.	1	Fully covered in the CHM process.	CHM4	no
		AI4.2	**AI4.2 Knowledge Transfer to Business Management** Transfer knowledge to business management to allow those individuals to take ownership of the system and data, and	1	Standard element of CHM process.	CHM6	no

			exercise responsibility for service delivery and quality, internal control, and application administration.				
		AI4.3	**AI4.3 Knowledge Transfer to End Users** Transfer knowledge and skills to allow end users to effectively and efficiently use the system in support of business processes.	1	Standard element of CHM process.	CHM6	no
		AI4.4	**AI4.4 Knowledge Transfer to Operations and Support Staff** Transfer knowledge and skills to enable operations and technical support staff to effectively and efficiently deliver, support and maintain the system and associated infrastructure.	1	Standard element of CHM process.	CHM6	no
	AI5 Procure IT resources	**AI5.1**	**AI5.1 Procurement Control** Develop and follow a set of procedures and standards that is consistent with the business organisation's overall procurement process and acquisition strategy to acquire IT-related infrastructure, facilities, hardware, software and services needed by the business.	2	Standard element of CHM process, but on a work-instruction level. Part of the Build step in CHM	CHM4	no
		AI5.2	**AI5.2 Supplier Contract Management** Set up a procedure for establishing, modifying and terminating contracts for all suppliers. The procedure should cover, at a minimum, legal, financial, organisational, documentary, performance, security, intellectual property, and termination responsibilities and liabilities (including penalty clauses). All contracts and contract changes should be reviewed by legal advisors.	3	Supplier Management is allocated as a task for SLM, but not specified in ISM.		no
		AI5.3	**AI5.3 Supplier Selection** Select suppliers according to a fair and formal practice to ensure a viable best fit based on specified requirements. Requirements should be optimised with input from potential suppliers.	3	Supplier Management is allocated as a task for SLM, but not specified in ISM.		no
		AI5.4	**AI5.4 IT Resources Acquisition** Protect and enforce the organisation's interests in all acquisition contractual agreements, including the rights and obligations of all parties in the contractual terms for the acquisition of software, development resources, infrastructure and services.	3	Can be supported at local work-instruction level in SLM and CHM.		no
	AI6 Manage changes	**AI6.1**	**AI6.1 Change Standards and Procedures** Set up formal change management procedures to handle in a standardised manner all requests (including maintenance and patches) for changes to applications, procedures, processes, system and service parameters, and the underlying platforms.	1	Fully covered in the CHM process.	CHM	yes
		AI6.2	**AI6.2 Impact Assessment, Prioritisation and Authorisation** Assess all requests for change in a structured way to determine the impact on the operational system and its functionality. Ensure that changes are categorised, prioritised and authorised.	1	Fully covered in the CHM process.	CHM	yes
		AI6.3	**AI6.3 Emergency Changes** Establish a process for defining, raising, testing, documenting, assessing and authorising emergency changes that do not follow the established change process.	1	Fully covered in the CHM process. NB: urgent changes are changes with the highest priority. The process will always follow the standard process flow, but at procedure level some changes may apply. This is a local organizational aspect.	CHM1.4	yes

		AI6.4	**AI6.4 Change Status Tracking and Reporting** Establish a tracking and reporting system to document rejected changes, communicate the status of approved and in-process changes, and complete changes. Make certain that approved changes are implemented as planned.	1	Fully covered in the CHM process.	CHM	yes
		AI6.5	**AI6.5 Change Closure and Documentation** Whenever changes are implemented, update the associated system and user documentation and procedures accordingly.	1	Fully covered in the CHM process.	CHM	yes
	AI7 Install and accredit solutions and changes	**AI7.1**	**AI7.1 Training** Train the staff members of the affected user departments and the operations group of the IT function in accordance with the defined training and implementation plan and associated materials, as part of every information systems development, implementation or modification project.	1	Standard element in the CHM process.	CHM4, CHM6	yes
		AI7.2	**AI7.2 Test Plan** Establish a test plan based on organisationwide standards that defines roles, responsibilities, and entry and exit criteria. Ensure that the plan is approved by relevant parties.	1	Standard element in the CHM process.	CHM5	yes
		AI7.3	**AI7.3 Implementation Plan** Establish an implementation and fallback/backout plan. Obtain approval from relevant parties.	1	Standard element in the CHM process.	CHM4	yes
		AI7.4	**AI7.4 Test Environment** Define and establish a secure test environment representative of the planned operations environment relative to security, internal controls, operational practices, data quality and privacy requirements, and workloads.	1	Standard element in the CHM process.	CHM5	yes
		AI7.5	**AI7.5 System and Data Conversion** Plan data conversion and infrastructure migration as part of the organisation's development methods, including audit trails, rollbacks and fallbacks.	1	Standard element in the CHM process.	CHM	yes
		AI7.6	**AI7.6 Testing of Changes** Test changes independently in accordance with the defined test plan prior to migration to the operational environment. Ensure that the plan considers security and performance.	1	Standard element in the CHM process.	CHM5	yes
		AI7.7	**AI7.7 Final Acceptance Test** Ensure that business process owners and IT stakeholders evaluate the outcome of the testing process as determined by the test plan. Remediate significant errors identified in the testing process, having completed the suite of tests identified in the test plan and any necessary regression tests. Following evaluation, approve promotion to production.	1	Standard element in the CHM process.	CHM5	yes
		AI7.8	**AI7.8 Promotion to Production** Following testing, control the handover of the changed system to operations, keeping it in line with the implementation plan. Obtain approval of the key stakeholders, such as users, system owner and operational management. Where appropriate, run the system in parallel with the old system for a while, and compare behaviour and results.	1	Standard element in the CHM process.	CHM5, CHM6	yes
		AI7.9	**AI7.9 Post-implementation Review** Establish procedures in line with the organisational change management standards to require a post-implementation review as set out in the implementation plan.	1	Standard element in the CHM process.	CHM6, CHM7	yes

Deliver and Support	**DS1 Define and manage service levels**	**DS1.1**	**DS1.1 Service Level Management Framework** Define a framework that provides a formalised service level management process between the customer and service provider. The framework should maintain continuous alignment with business requirements and priorities and facilitate common understanding between the customer and provider(s). The framework should include processes for creating service requirements, service definitions, SLAs, OLAs and funding sources. These attributes should be organised in a service catalogue. The framework should define the organisational structure for service level management, covering the roles, tasks and responsibilities of internal and external service providers and customers.	1	Fully covered by the SLM process. NB: organizational structures are always local issues. These are supported in the ISM publishing tool. ISM contains templates for standardized SLAs, OLAs, and service catalogs.	SLM	yes
		DS1.2	**DS1.2 Definition of Services** Base definitions of IT services on service characteristics and business requirements. Ensure that they are organised and stored centrally via the implementation of a service catalogue portfolio approach.	1	Fully covered by the SLM process.	SLM	yes
		DS1.3	**DS1.3 Service Level Agreements** Define and agree to SLAs for all critical IT services based on customer requirements and IT capabilities. This should cover customer commitments; service support requirements; quantitative and qualitative metrics for measuring the service signed off on by the stakeholders; funding and commercial arrangements, if applicable; and roles and responsibilities, including oversight of the SLA. Consider items such as availability, reliability, performance, capacity for growth, levels of support, continuity planning, security and demand constraints.	1	Fully covered by the SLM process. ISM contains templates for standardized SLAs.	SLM	yes
		DS1.4	**DS1.4 Operating Level Agreements** Define OLAs that explain how the services will be technically delivered to support the SLA(s) in an optimal manner. The OLAs should specify the technical processes in terms meaningful to the provider and may support several SLAs.	1	Fully covered by the SLM process. ISM contains templates for standardized OLAs.	SLM	yes
		DS1.5	**DS1.5 Monitoring and Reporting of Service Level Achievements** Continuously monitor specified service level performance criteria. Reports on achievement of service levels should be provided in a format that is meaningful to the stakeholders. The monitoring statistics should be analysed and acted upon to identify negative and positive trends for individual services as well as for services overall.	1	Fully covered by the OM process (Monitoring) and the SLM process (reporting to customer).	SLM, OM	yes
		DS1.6	**DS1.6 Review of Service Level Agreements and Contracts** Regularly review SLAs and underpinning contracts (UCs) with internal and external service providers to ensure that they are effective and up to date and that changes in requirements have been taken into account.	1	Fully covered by the SLM process.	SLM	yes
	DS2 Manage third-party services	**DS2.1**	**DS2.1 Identification of All Supplier Relationships** Identify all supplier services, and categorise them according to supplier type, significance and criticality. Maintain formal documentation of technical and organisational relationships covering the roles and responsibilities, goals, expected deliverables, and credentials of representatives of these suppliers.	2	Supplier contracts are taken into account during the creation of a new or updated SLA. These contracts are registered in the implementation phase of the new/updated service. All organizational roles are registered in the process-publishing tool.	SLM1.5; SLM2.1	no

		DS2.2	**DS2.2 Supplier Relationship Management** Formalise the supplier relationship management process for each supplier. The relationship owners should liaise on customer and supplier issues and ensure the quality of the relationship based on trust and transparency (e.g., through SLAs).	2	See DS2.1. A supplier can contribute to various processes. E.g. to the planning and implementaion of a change, or to the resolution of an incident.	SLM1.5, CHM3.1, IM2.3	no
		DS2.3	**DS2.3 Supplier Risk Management** Identify and mitigate risks relating to suppliers' ability to continue effective service delivery in a secure and efficient manner on a continual basis. Ensure that contracts conform to universal business standards in accordance with legal and regulatory requirements. Risk management should further consider non-disclosure agreements (NDAs), escrow contracts, continued supplier viability, conformance with security requirements, alternative suppliers, penalties and rewards, etc.	2	This is subject to the standard QM process, and can be covered at work-instruction level.	QM	no
		DS2.4	**DS2.4 Supplier Performance Monitoring** Establish a process to monitor service delivery to ensure that the supplier is meeting current business requirements and continuing to adhere to the contract agreements and SLAs, and that performance is competitive with alternative suppliers and market conditions.	2	This is subject to the standard OM2 Monitoring sub-process, and can be covered at work-instruction level.	OM2	no
	DS3 Manage performance and capacity	**DS3.1**	**DS3.1 Performance and Capacity Planning** Establish a planning process for the review of performance and capacity of IT resources to ensure that cost-justifiable capacity and performance are available to process the agreed-upon workloads as determined by the SLAs. Capacity and performance plans should leverage appropriate modelling techniques to produce a model of the current and forecasted performance, capacity and throughput of the IT resources.	2	Covered in the OM process. Regular performance and capacity releated tasks are planned and executed in OM1 and all performance and capacity related items are monitored in OM2 Techniques are subject to work-instruction levels.	OM1, OM2	yes
		DS3.2	**DS3.2 Current Performance and Capacity** Assess current performance and capacity of IT resources to determine if sufficient capacity and performance exist to deliver against agreed-upon service levels.	1	Covered in OM2 Monitoring	OM2	yes
		DS3.3	**DS3.3 Future Performance and Capacity** Conduct performance and capacity forecasting of IT resources at regular intervals to minimise the risk of service disruptions due to insufficient capacity or performance degradation, and identify excess capacity for possible redeployment. Identify workload trends and determine forecasts to be input to performance and capacity plans.	2	The data from the ISM processes feed this activity, e.g. QM discovers the risks of not delivering against agreed service levels, and also inefficient use of resources. The QM1.1 step determines risks based on workload trends, based on data from OM2 Monitoring.	OM2, QM1.1	yes
		DS3.4	**DS3.4 IT Resources Availability** Provide the required capacity and performance, taking into account aspects such as normal workloads, contingencies, storage requirements and IT resource life cycles. Provisions such as prioritising tasks, fault-tolerance mechanisms and resource allocation practices should be made. Management should ensure that contingency plans properly address availability, capacity and performance of individual IT resources.	2	Covered in OM1 Contingency plans can be detailed at work-instruction level.	OM1	yes

		DS3.5	**DS3.5 Monitoring and Reporting** Continuously monitor the performance and capacity of IT resources. Data gathered should serve two purposes: • To maintain and tune current performance within IT and address such issues as resilience, contingency, current and projected workloads, storage plans, and resource acquisition • To report delivered service availability to the business, as required by the SLAs Accompany all exception reports with recommendations for corrective action.	1	Fully covered in OM2	OM2	yes
	DS4 Ensure continuous service	**DS4.1**	**DS4.1 IT Continuity Framework** Develop a framework for IT continuity to support enterprisewide business continuity management using a consistent process. The objective of the framework should be to assist in determining the required resilience of the infrastructure and to drive the development of disaster recovery and IT contingency plans. The framework should address the organisational structure for continuity management, covering the roles, tasks and responsibilities of internal and external service providers, their management and their customers, and the planning processes that create the rules and structures to document, test and execute the disaster recovery and IT contingency plans. The plan should also address items such as the identification of critical resources, noting key dependencies, the monitoring and reporting of the availability of critical resources, alternative processing, and the principles of backup and recovery.	2	Covered in the ISM framework. In SLM1.2 the translation to a Service Specsheet is made, and in SLM1.3 the feasability of the specs is verified. This covers the translation into operational requirements like backup and recovery, and any other continuity measures. The Publishing Tool covers the integration with organizational structures. Risks and disaster recovery plans are subject to the QM process. Disaster recovery plans are managed at various positions in the CHM process. Critical resources are identified in the QM process. Monitoring plans are covered in the OM2 sub process. All continuity infrastructure is registered in the CMDB. Recovery from minor and major disturbances is covered in the IM process.	SLM1.3, QM, CHM, OM2, COM, IM	yes
		DS4.2	**DS4.2 IT Continuity Plans** Develop IT continuity plans based on the framework and designed to reduce the impact of a major disruption on key business functions and processes. The plans should be based on risk understanding of potential business impacts and address requirements for resilience, alternative processing and recovery capability of all critical IT services. They should also cover usage guidelines, roles and responsibilities, procedures, communication processes, and the testing approach.	2	Covered throughout the ISM Framework, see DS4.1	SLM, QM, CHM, IM, OM, COM	yes
		DS4.3	**DS4.3 Critical IT Resources** Focus attention on items specified as most critical in the IT continuity plan to build in resilience and establish priorities in recovery situations. Avoid the distraction of recovering less-critical items and ensure response and recovery in line with prioritised business needs, while ensuring that costs are kept at an acceptable level and complying with regulatory and contractual requirements. Consider resilience, response and recovery requirements for different tiers, e.g., one to four hours, four to 24 hours, more than 24 hours and critical business operational periods.	2	Covered throughout the ISM Framework, see DS4.1	SLM, QM, CHM, IM, OM, COM	yes
		DS4.4	**DS4.4 Maintenance of the IT Continuity Plan** Encourage IT management to define and execute change control procedures to ensure that the IT continuity plan is kept up to date and continually reflects actual business	1	Covered throughout the CH process.	CHM	yes

			requirements. Communicate changes in procedures and responsibilities clearly and in a timely manner.				
		DS4.5	**DS4.5 Testing of the IT Continuity Plan** Test the IT continuity plan on a regular basis to ensure that IT systems can be effectively recovered, shortcomings are addressed and the plan remains relevant. This requires careful preparation, documentation, reporting of test results and, according to the results, implementation of an action plan. Consider the extent of testing recovery of single applications to integrated testing scenarios to end-to-end testing and integrated vendor testing.	1	This is covered in the OM1 sub process. Details are covered at work-instruction level. Testing can be triggered from a variety of sources, e.g. in case a change is heavily influencing a continuity plan, or because QM has registered a specific risk that needs to be counteracted.	OM1	yes
		DS4.6	**DS4.6 IT Continuity Plan Training** Provide all concerned parties with regular training sessions regarding the procedures and their roles and responsibilities in case of an incident or disaster. Verify and enhance training according to the results of the contingency tests.	2	Covered in OM1, at work-instruction level.	OM1	yes
		DS4.7	**DS4.7 Distribution of the IT Continuity Plan** Determine that a defined and managed distribution strategy exists to ensure that plans are properly and securely distributed and available to appropriately authorised interested parties when and where needed. Attention should be paid to making the plans accessible under all disaster scenarios.	2	Covered in OM1, at work-instruction level. The CHM process makes sure that registration in COM is planned and implemented.	OM1, CHM, COM	yes
		DS4.8	**DS4.8 IT Services Recovery and Resumption** Plan the actions to be taken for the period when IT is recovering and resuming services. This may include activation of backup sites, initiation of alternative processing, customer and stakeholder communication, and resumption procedures. Ensure that the business understands IT recovery times and the necessary technology investments to support business recovery and resumption needs.	2	This is an element of the disaster recovery plan (IT Continuity Plan), see DS4.2	SLM, QM, CHM, IM, OM, COM	yes
		DS4.9	**DS4.9 Offsite Backup Storage** Store offsite all critical backup media, documentation and other IT resources necessary for IT recovery and business continuity plans. Determine the content of backup storage in collaboration between business process owners and IT personnel. Management of the offsite storage facility should respond to the data classification policy and the enterprise's media storage practices. IT management should ensure that offsite arrangements are periodically assessed, at least annually, for content, environmental protection and security. Ensure compatibility of hardware and software to restore archived data, and periodically test and refresh archived data.	2	Covered throughout the ISM Framework, see DS4.1	SLM, QM, CHM, IM, OM, COM	yes
		DS4.10	**DS4.10 Post-resumption Review** Determine whether IT management has established procedures for assessing the adequacy of the plan in regard to the successful resumption of the IT function after a disaster, and update the plan accordingly.	2	Covered throughout the ISM Framework, see DS4.1	SLM, QM, CHM, IM, OM, COM	yes

	DS5 Ensure systems security	**DS5.1**	**DS5.1 Management of IT Security** Manage IT security at the highest appropriate organisational level, so the management of security actions is in line with business requirements.	1	Covered throughout the ISM Framework. SLM covers service security levels in the Security paragraph of the SLA. Security risks are handles in QM Security changes are handled in CHM, and all changes are assessed in terms of security, involving the security manager. Security incidents are handled in the IM process. Security is delivered according to agreed service levels in Planning & Scheduling, and all services are monitored against these agreed service levels. All security infrastructure components are registered in COM.	SLM, QM, CHM, IM, OM, COM	yes
		DS5.2	**DS5.2 IT Security Plan** Translate business, risk and compliance requirements into an overall IT security plan, taking into consideration the IT infrastructure and the security culture. Ensure that the plan is implemented in security policies and procedures together with appropriate investments in services, personnel, software and hardware. Communicate security policies and procedures to stakeholders and users.	2	In SLM1.2 the translation to a Service Specsheet is made, and in SLM1.3 the feasability of the specs is verified. QM can set general requirements to an overall security plan that is used in OM, in CHM, in OM and in IM	SLM, QM, CHM, IM, OM, COM	yes
		DS5.3	**DS5.3 Identity Management** Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms. Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the security-responsible person. Maintain user identities and access rights in a central repository. Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implementauthentication and enforce access rights.	2	This is a requirement in the SLA, that is implemented through CHM in OM, and in IM As usual, QM will determine risks that threaten this, and COM will register whatever infractructural elements are used to accomplish this. Requests for identities are normally handled as service requests.	SLM, QM, CHM, IM, OM, COM	yes
		DS5.4	**DS5.4 User Account Management** Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.	2	This is a requirement in the SLA, that is implemented through CHM in OM, and in IM As usual, QM will determine risks that threaten this, and COM will register whatever infractructural elements are used to accomplish this. Requests for user accounts are normally handled as service requests.	SLM, QM, CHM, IM, OM, COM	yes
		DS5.5	**DS5.5 Security Testing, Surveillance and Monitoring** Test and monitor the IT security implementation in a proactive way. IT security should be reaccredited in a timely manner to ensure that the approved enterprise's information security baseline is maintained. A logging and monitoring	2	The implemented IT security is tested before implementation in the CHM process. After implementaion it is monitored in OM2 All requirements can be set by SLM and by QM	CHM, OM2, QM, IM	yes

			function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.		Security incidents will be handled through IM		
		DS5.6	**DS5.6 Security Incident Definition** Clearly define and communicate the characteristics of potential security incidents so they can be properly classified and treated by the incident and problem management process.	2	Handling security incidents is covered in the IM process. Security risks ('problems') are handled in the QM process.	IM, QM	yes
		DS5.7	**DS5.7 Protection of Security Technology** Make security-related technology resistant to tampering, and do not disclose security documentation unnecessarily.	2	Covered in the OM1 sub process, as agreed/specified in earlier steps (in SLM, through CHM, and based on the specifications from all relevant sources in the organization).	OM1	yes
		DS5.8	**DS5.8 Cryptographic Key Management** Determine that policies and procedures are in place to organise the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorised disclosure.	2	Covered in the OM1 sub process, as agreed/specified in earlier steps (in SLM, through CHM, and based on the specifications from all relevant sources in the organization).	OM1	yes
		DS5.9	**DS5.9 Malicious Software Prevention, Detection and Correction** Put preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the organisation to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).	2	Covered in the OM1 sub process, as agreed/specified in earlier steps (in SLM, through CHM, and based on the specifications from all relevant sources in the organization).	OM1	yes
		DS5.10	**DS5.10 Network Security** Use security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation, intrusion detection) to authorise access and control information flows from and to networks.	2	Covered in the OM1 sub process, as agreed/specified in earlier steps (in SLM, through CHM, and based on the specifications from all relevant sources in the organization).	OM1	yes
		DS5.11	**DS5.11 Exchange of Sensitive Data** Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin.	2	Covered in the OM1 sub process, as agreed/specified in earlier steps (in SLM, through CHM, and based on the specifications from all relevant sources in the organization).	OM1	yes
	DS6 Identify and allocate costs	**DS6.1**	**DS6.1 Definition of Services** Identify all IT costs, and map them to IT services to support a transparent cost model. IT services should be linked to business processes such that the business can identify associated service billing levels.	2	Covered throughout the ISM framework. SLM covers costs of services in the Financial paragraph of the SLA. Financial risks (e.g. discrepancies between forecasts and agreed cost levels) are handles in QM Finance changes are handled in CHM, and all changes are assessed in terms of costing and charging. Finance incidents are handled in the IM process. All financial infrastructure components are registered in COM Financial entities like invoices are produced in the OM1 sub process. All finance service levels(consumption, cost) are monitored in OM2	SLM, QM, CHM, IM, OM, COM	no

		DS6.2	**DS6.2 IT Accounting** Capture and allocate actual costs according to the enterprise cost model. Variances between forecasts and actual costs should be analysed and reported on, in compliance with the enterprise's financial measurement systems.	2	See DS6.1	SLM, QM, CHM, IM, OM, COM	no
		DS6.3	**DS6.3 Cost Modelling and Charging** Establish and use an IT costing model based on the service definitions that support the calculation of chargeback rates per service. The IT cost model should ensure that charging for services is identifiable, measurable and predictable by users to encourage proper use of resources.	2	See DS6.1	SLM, QM, CHM, IM, OM, COM	no
		DS6.4	**DS6.4 Cost Model Maintenance** Regularly review and benchmark the appropriateness of the cost/recharge model to maintain its relevance and appropriateness to the evolving business and IT activities.	2	See DS6.1	SLM, QM, CHM, IM, OM, COM	no
	DS7 Educate and train users	**DS7.1**	**DS7.1 Identification of Education and Training Needs** Establish and regularly update a curriculum for each target group of employees considering: • Current and future business needs and strategy • Value of information as an asset • Corporate values (ethical values, control and security culture, etc.) • Implementation of new IT infrastructure and software (i.e., packages, applications) • Current and future skills, competence profiles, and certification and/or credentialing needs as well as required reaccreditation • Delivery methods (e.g., classroom, web-based), target group size, accessibility and timing	2	Covered throughout the ISM framework. SLM covers training requirements as agreed in the SLA. Training (i.e. lack of) can be acknowledged as a risk in QM Training Planning changes are handled in CHM, and all changes are assessed in terms of training. Training incidents are handled in the IM process. All training infrastructure components are registered in COM Training is delivered in OM1 sub process. All training requirements can be monitored in OM2	SLM, QM, CHM, IM, OM, COM	no
		DS7.2	**DS7.2 Delivery of Training and Education** Based on the identified education and training needs, identify target groups and their members, efficient delivery mechanisms, teachers, trainers, and mentors. Appoint trainers and organise timely training sessions. Record registration (including prerequisites), attendance and training session performance evaluations.	2	See DS7.1	SLM, QM, CHM, IM, OM, COM	no
		DS7.3	**DS7.3 Evaluation of Training Received** Evaluate education and training content delivery upon completion for relevance, quality, effectiveness, the retention of knowledge, cost and value. The results of this evaluation should serve as input for future curriculum definition and the delivery of training sessions.	2	See DS7.1	SLM, QM, CHM, IM, OM, COM	no
	DS8 Manage service desk and incidents	**DS8.1**	**DS8.1 Service Desk** Establish a service desk function, which is the user interface with IT, to register, communicate, dispatch and analyse all calls, reported incidents, service requests and information demands. There should be monitoring and escalation procedures based on agreed-upon service levels relative to the appropriate SLA that allow classification and prioritisation of any reported issue as an incident, service request or information request. Measure end users' satisfaction with the quality of the service desk and IT services.	2	Covered throughout the ISM framework. SLM covers the availability and requirements of a Service desk as agreed in the SLA. Service Desk risks are handled in QM Service Desk changes are handled in CHM, and all changes are assessed in terms of involving the Service Desk Service desk incidents are handled in the IM process. All Service desk infrastructure components are registered in COM The Service Desk deliveres operational	SLM, QM, CHM, IM, OM, COM	yes

					services in the OM1 sub process, and all monitoring in OM2		
		DS8.2	**DS8.2 Registration of Customer Queries** Establish a function and system to allow logging and tracking of calls, incidents, service requests and information needs. It should work closely with such processes as incident management, problem management, change management, capacity management and availability management. Incidents should be classified according to a business and service priority and routed to the appropriate problem management team, where necessary. Customers should be kept informed of the status of their queries.	2	Covered throughout the ISM framework. Re system: customer queries are either: 1- requests to change the services, or complaints about the contracts. These are handled in SLM 2- requests to change the delivered services, as agreed in an SLA. These are hadled in CHM 3- requests to resolve disturbances to the agreed services. These are handled in IM 4- requests to deliver service volumes or information needs as specified in the SLA. These are handled in OM1. Re function: customer calls can be handled by a Service Desk or any other function or functions. E.g., requests to change SLAs are normall addressed to account managers or service managers, and these roles are not necessarily covered by the Service Desk.	SLM, CHM, IM, OM	yes
		DS8.3	**DS8.3 Incident Escalation** Establish service desk procedures, so incidents that cannot be resolved immediately are appropriately escalated according to limits defined in the SLA and, if appropriate, workarounds are provided. Ensure that incident ownership and life cycle monitoring remain with the service desk for user-based incidents, regardless which IT group is working on resolution activities.	2	Covered in IM If a Service Desk is defined, this can be covered in detail in the Publishing Tool, and at procedure/work-instruction level.	SLM, QM, CHM, IM, OM, COM	yes
		DS8.4	**DS8.4 Incident Closure** Establish procedures for the timely monitoring of clearance of customer queries. When the incident has been resolved, ensure that the service desk records the resolution steps, and confirm that the action taken has been agreed to by the customer. Also record and report unresolved incidents (known errors and workarounds) to provide information for proper problem management.	1	Covered in IM, in IM0 Process Control, and in IM5 and IM6. A Service Desk is an optional function in an organization.	IM	yes
		DS8.5	**DS8.5 Reporting and Trend Analysis** Produce reports of service desk activity to enable management to measure service performance and service response times and to identify trends or recurring problems, so service can be continually improved.	2	All reporting is covered in the relevant ISM process. A Service Desk is an optional function in an organization.	SLM, QM, CHM, IM, OM, COM	yes
	DS9 Manage the configuration	**DS9.1**	**DS9.1 Configuration Repository and Baseline** Establish a supporting tool and a central repository to contain all relevant information on configuration items. Monitor and record all assets and changes to assets. Maintain a baseline of configuration items for every system and service as a	1	Registration is covered in COM2 The CHM proces makes sure that no changes are applied to registered infrastructure componets, unless through the CHM process, involving COM	CHM, COM	yes

			checkpoint to which to return after changes.		Baselines and roll-back plans are covered in CHM4.1		
		DS9.2	**DS9.2 Identification and Maintenance of Configuration Items** Establish configuration procedures to support management and logging of all changes to the configuration repository. Integrate these procedures with change management, incident management and problem management procedures.	1	This is covered throughout ISM. The CHM proces makes sure that no changes are applied to registered infrastructure componets, unless through the CHM process, involving COM In case a configuration needs to be changed when resolving an incident in IM, this is run through CHM In case a risk needs to be resolved in QM, through a change to the configuration, this is run through CHM In case COM3 detects errors in the configuration during a configuration audit, the resulting change is run through CHM In case a CMDB error is detected, the administration is repaired.	COM, CHM, IM, QM	yes
		DS9.3	**DS9.3 Configuration Integrity Review** Periodically review the configuration data to verify and confirm the integrity of the current and historical configuration. Periodically review installed software against the policy for software usage to identify personal or unlicensed software or any software instances in excess of current license agreements. Report, act on and correct errors and deviations.	1	Fully covered in OM3	OM3	yes
	DS10 Manage problems	**DS10.1**	**DS10.1 Identification and Classification of Problems** Implement processes to report and classify problems that have been identified as part of incident management. The steps involved in problem classification are similar to the steps in classifying incidents; they are to determine category, impact, urgency and priority. Categorise problems as appropriate into related groups or domains (e.g., hardware, software, support software). These groups may match the organisational responsibilities of the user and customer base, and should be the basis for allocating problems to support staff.	1	Fully covered in QM Exception: incidents are NOT promoted to problems. This is a conbceptual error.	QM	yes
		DS10.2	**DS10.2 Problem Tracking and Resolution** Ensure that the problem management system provides for adequate audit trail facilities that allow tracking, analysing and determining the root cause of all reported problems considering: • All associated configuration items • Outstanding problems and incidents • Known and suspected errors • Tracking of problem trends Identify and initiate sustainable solutions addressing the root cause, raising change requests via the established change management process. Throughout the resolution process, problem management should obtain regular reports from change management on progress in resolving problems and errors. Problem management should monitor the continuing impact of problems and known errors on user services. In the event that this impact becomes severe, problem management	1	Fully covered in QM and CHM OM2 monitors everything QM requires.	QM, CHM	yes

			should escalate the problem, perhaps referring it to an appropriate board to increase the priority of the (RFC or to implement an urgent change as appropriate. Monitor the progress of problem resolution against SLAs.				
		DS10.3	**DS10.3 Problem Closure** Put in place a procedure to close problem records either after confirmation of successful elimination of the known error or after agreement with the business on how to alternatively handle the problem.	1	Fully covered in QM5	QM5	yes
		DS10.4	**DS10.4 Integration of Configuration, Incident and Problem Management** Integrate the related processes of configuration, incident and problem management to ensure effective management of problems and enable improvements.	1	Fully covered in the integrated process model of ISM. QM can be triggered by data from IM and COM	IM, COM, QM	yes
	DS11 Manage data	**DS11.1**	**DS11.1 Business Requirements for Data Management** Verify that all data expected for processing are received and processed completely, accurately and in a timely manner, and all output is delivered in accordance with business requirements. Support restart and reprocessing needs.	2	Fully covered in OM2 and IM	OM2, IM	yes
		DS11.2	**DS11.2 Storage and Retention Arrangements** Define and implement procedures for effective and efficient data storage, retention and archiving to meet business objectives, the organisation's security policy and regulatory requirements.	2	Fully covered in OM1, as agreed in SLAs and in internal policies.	OM1	yes
		DS11.3	**DS11.3 Media Library Management System** Define and implement procedures to maintain an inventory of stored and archived media to ensure their usability and integrity.	2	Fully covered in OM1, as agreed in SLAs and in internal policies. Changes to the Media Library Management system are run through CHM, and all content of the system is registered in COM	OM1, CHM, COM	yes
		DS11.4	**DS11.4 Disposal** Define and implement procedures to ensure that business requirements for protection of sensitive data and software are met when data and hardware are disposed or transferred.	2	Fully covered in OM1, as agreed in SLAs and in internal policies.	OM1	yes
		DS11.5	**DS11.5 Backup and Restoration** Define and implement procedures for backup and restoration of systems, applications, data and documentation in line with business requirements and the continuity plan.	2	Fully covered in OM1, as agreed in SLAs and in internal policies.	OM1	yes
		DS11.6	**DS11.6 Security Requirements for Data Management** Define and implement policies and procedures to identify and apply security requirements applicable to the receipt, processing, storage and output of data to meet business objectives, the organisation's security policy and regulatory requirements.	2	Fully covered in the relevant ISM processes. See DS5.	SLM, QM, CHM, IM, OM, COM	yes

	DS12 Manage the physical environment	**DS12.1**	**DS12.1 Site Selection and Layout** Define and select the physical sites for IT equipment to support the technology strategy linked to the business strategy. The selection and design of the layout of a site should take into account the risk associated with natural and man-made disasters, whilst considering relevant laws and regulations, such as occupational health and safety regulations.	2	Fully covered in OM1, as agreed in SLAs and in internal policies. Risks are handled by QM	OM1, QM	yes
		DS12.2	**DS12.2 Physical Security Measures** Define and implement physical security measures in line with business requirements to secure the location and the physical assets. Physical security measures must be capable of effectively preventing, detecting and mitigating risks relating to theft, temperature, fire, smoke, water, vibration, terror, vandalism, power outages, chemicals or explosives.	2	Fully covered in OM1, as agreed in SLAs and in internal policies. Risks are handled by QM	OM1, QM	yes
		DS12.3	**DS12.3 Physical Access** Define and implement procedures to grant, limit and revoke access to premises, buildings and areas according to business needs, including emergencies. Access to premises, buildings and areas should be justified, authorised, logged and monitored. This should apply to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party.	2	Fully covered in OM1, as agreed in SLAs and in internal policies. Monitoring is handled in OM2	OM1, OM2,	yes
		DS12.4	**DS12.4 Protection Against Environmental Factors** Design and implement measures for protection against environmental factors. Install specialised equipment and devices to monitor and control the environment.	2	Fully covered in OM1, as agreed in SLAs and in internal policies. Risks are handled by QM Protective measures are implemented through CHM Monitoring is handled in OM2	OM1, OM2, QM, CHM	yes
		DS12.5	**DS12.5 Physical Facilities Management** Manage facilities, including power and communications equipment, in line with laws and regulations, technical and business requirements, vendor specifications, and health and safety guidelines.	2	Fully covered in OM1, as agreed in SLAs and in internal policies. Monitoring is handled in OM2	OM1, OM2,	yes
	DS13 Manage operations	**DS13.1**	**DS13.1 Operations Procedures and Instructions** Define, implement and maintain procedures for IT operations, ensuring that the operations staff members are familiar with all operations tasks relevant to them. Operational procedures should cover shift handover (formal handover of activity, status updates, operational problems, escalation procedures and reports on current responsibilities) to support agreed-upon service levels and ensure continuous operations.	2	Fully covered in OM1, as agreed in SLAs and in internal policies.	OM1	yes
		DS13.2	**DS13.2 Job Scheduling** Organise the scheduling of jobs, processes and tasks into the most efficient sequence, maximising throughput and utilisation to meet business requirements.	1	Fully covered in OM1, as agreed in SLAs and in internal policies.	OM1	yes
		DS13.3	**DS13.3 IT Infrastructure Monitoring** Define and implement procedures to monitor the IT infrastructure and related events. Ensure that sufficient chronological information is being stored in operations logs to enable the reconstruction, review and examination of the time sequences of operations and the other activities surrounding or supporting operations.	2	Fully covered in OM2, as agreed in SLAs and in internal policies.	OM2	yes
		DS13.4	**DS13.4 Sensitive Documents and Output Devices** Establish appropriate physical safeguards, accounting practices and inventory management over sensitive IT assets,	2	Fully covered in OM1, as agreed in SLAs and in internal policies.	OM1	yes

			such as special forms, negotiable instruments, special purpose printers or security tokens.				
		DS13.5	**DS13.5 Preventive Maintenance for Hardware** Define and implement procedures to ensure timely maintenance of infrastructure to reduce the frequency and impact of failures or performance degradation.	2	Fully covered in OM1, as agreed in SLAs and in internal policies. Risks towards hardware are handled in QM	OM1, QM	yes
Monitor and Evaluate	**ME1 Monitor and evaluate IT performance**	**ME1.1**	**ME1.1 Monitoring Approach** Establish a general monitoring framework and approach to define the scope, methodology and process to be followed for measuring IT's solution and service delivery, and monitor IT's contribution to the business. Integrate the framework with the corporate performance management system.	1	Fully covered in OM2 SLAs are the interface with the corporate performance management system.	OM2	no
		ME1.2	**ME1.2 Definition and Collection of Monitoring Data** Work with the business to define a balanced set of performance targets and have them approved by the business and other relevant stakeholders. Define benchmarks with which to compare the targets, and identify available data to be collected to measure the targets. Establish processes to collect timely and accurate data to report on progress against targets.	2	Covered in OM2 Benchmarking is a management activity that can either be used in QM (covered in ISM) or as a decision support tool (outside of the scope of ISM).	OM2, QM	no
		ME1.3	**ME1.3 Monitoring Method** Deploy a performance monitoring method (e.g., balanced scorecard) that records targets; captures measurements; provides a succinct, all-around view of IT performance; and fits within the enterprise monitoring system.	2	Fully covered in OM2 Detailed methods are subject to work-instruction level.	OM2	no
		ME1.4	**ME1.4 Performance Assessment** Periodically review performance against targets, analyse the cause of any deviations, and initiate remedial action to address the underlying causes. At appropriate times, perform root cause analysis across deviations.	2	Fully covered in OM2 Events are either handled as incidents in IM, or handled in QM as a consequence of reporting data.	OM2, IM, QM	no
		ME1.5	**ME1.5 Board and Executive Reporting** Develop senior management reports on IT's contribution to the business, specifically in terms of the performance of the enterprise's portfolio, IT-enabled investment programmes, and the solution and service deliverable performance of individual programmes. Include in status reports the extent to which planned objectives have been achieved, budgeted resources used, set performance targets met and identified risks mitigated. Anticipate senior management's review by suggesting remedial actions for major deviations. Provide the report to senior management, and solicit feedback from management's review.	2	Covered in SLM2 All data and suggestions may be based upon lower-level reporting in functions and processes.	SLM2	no
		ME1.6	**ME1.6 Remedial Actions** Identify and initiate remedial actions based on performance monitoring, assessment and reporting. This includes follow-up of all monitoring, reporting and assessments through: • Review, negotiation and establishment of management responses • Assignment of responsibility for remediation • Tracking of the results of actions committed	2	Identification of events is covered in OM2. The analysis of logging data of OM2 can also lead to the discovery of risks in QM. Identified events are either logged as information, or treated as incidents in IM.	OM2, QM, IM	no

	ME2 Monitor and evaluate internal control	**ME2.1**	**ME2.1 Monitoring of Internal Control Framework** Continuously monitor, benchmark and improve the IT control environment and control framework to meet organisational objectives.	2	Fully covered by ISM. ISM is a control framework for the delivery of quality services as agreed in SLAs. Each ISM process has a Control Process that continuously monitors the control environment. Benchmarking is not within the specific scope, but can be an instrument at work-instruction level.	ISM	no
		ME2.2	**ME2.2 Supervisory Review** Monitor and evaluate the efficiency and effectiveness of internal IT managerial review controls.	2	Fully covered by ISM. Each ISM process has a Control Process that continuously monitors the control environment.	ISM	no
		ME2.3	**ME2.3 Control Exceptions** Identify control exceptions, and analyse and identify their underlying root causes. Escalate control exceptions and report to stakeholders appropriately. Institute necessary corrective action.	2	See ME2.2	ISM	no
		ME2.4	**ME2.4 Control Self-assessment** Evaluate the completeness and effectiveness of management's control over IT processes, policies and contracts through a continuing programme of self-assessment.	4	ISM covers all six basic processes at operational and tactical level of an IT organization. It contains a control mechanism at the level of each process, and it has its own QM process for quality improvement and risk management. Self-assessment is an optional technique not explicitly covered in ISM.		no
		ME2.5	**ME2.5 Assurance of Internal Control** Obtain, as needed, further assurance of the completeness and effectiveness of internal controls through third-party reviews.	4	Third-party reviews are not part of the ISM framework.		no
		ME2.6	**ME2.6 Internal Control at Third Parties** Assess the status of external service providers' internal controls. Confirm that external service providers comply with legal and regulatory requirements and contractual obligations.	4	Out of scope		no
		ME2.7	**ME2.7 Remedial Actions** Identify, initiate, track and implement remedial actions arising from control assessments and reporting.	1	ISM has an over-all QM process to cover all improvements and risks. In SLM2 improvement plans are agreedwith customers. In OM2 meaning events are monitored, triggering resolutions through the IM process.	QM, SLM2, OM2, IM	no
	ME3 Ensure compliance with external requirements	**ME3.1**	**ME3.1 Identification of External Legal, Regulatory and Contractual Compliance Requirements** Identify, on a continuous basis, local and international laws, regulations, and other external requirements that must be complied with for incorporation into the organisation's IT policies, standards, procedures and methodologies.	2	QM covers identification of all gaps with requirements, internal and external.	QM	no
		ME3.2	**ME3.2 Optimisation of Response to External Requirements** Review and adjust IT policies, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated.	2	QM covers detection and handling of all risks, internal and external.	QM	no
		ME3.3	**ME3.3 Evaluation of Compliance With External Requirements** Confirm compliance of IT policies, standards, procedures and	2	This is the result of ME3.1, covered by QM	QM	no

			methodologies with legal and regulatory requirements.				
		ME3.4	**ME3.4 Positive Assurance of Compliance** Obtain and report assurance of compliance and adherence to all internal policies derived from internal directives or external legal, regulatory or contractual requirements, confirming that any corrective actions to address any compliance gaps have been taken by the responsible process owner in a timely manner.	2	Fully covered by QM	QM	no
		ME3.5	**ME3.5 Integrated Reporting** Integrate IT reporting on legal, regulatory and contractual requirements with similar output from other business functions.	4	Out of scope		no
	ME4 Provide IT governance	**ME4.1**	**ME4.1 Establishment of an IT Governance Framework** Define, establish and align the IT governance framework with the overall enterprise governance and control environment. Base the framework on a suitable IT process and control model and provide for unambiguous accountability and practices to avoid a breakdown in internal control and oversight. Confirm that the IT governance framework ensures compliance with laws and regulations and is aligned with, and confirms delivery of, the enterprise's strategies and objectives. Report IT governance status and issues.	2	Fully covered by the ISM framework. The integrated process model is an essentia element of the framework. The Publishing Tool determines the entire set of RACI (RASCI, FURI) relationships to roles and people in the organization. The QM process discovers risks of non-compliance natureand handles them.	ISM	no
		ME4.2	**ME4.2 Strategic Alignment** Enable board and executive understanding of strategic IT issues, such as the role of IT, technology insights and capabilities. Ensure that there is a shared understanding between the business and IT regarding the potential contribution of IT to the business strategy. Work with the board and the established governance bodies, such as an IT strategy committee, to provide strategic direction to management relative to IT, ensuring that the strategy and objectives are cascaded into business units and IT functions, and that confidence and trust are developed between the business and IT. Enable the alignment of IT to the business in strategy and operations, encouraging co-responsibility between the business and IT for making strategic decisions and obtaining benefits from IT-enabled investments.	4	Out of scope		no
		ME4.3	**ME4.3 Value Delivery** Manage IT-enabled investment programmes and other IT assets and services to ensure that they deliver the greatest possible value in supporting the enterprise's strategy and objectives. Ensure that the expected business outcomes of IT-enabled investments and the full scope of effort required to achieve those outcomes are understood; that comprehensive and consistent business cases are created and approved by stakeholders; that assets and investments are managed throughout their economic life cycle; and that there is active management of the realisation of benefits, such as contribution to new services, efficiency gains and improved responsiveness to customer demands. Enforce a disciplined approach to portfolio, programme and project management, insisting that the business takes ownership of all IT-enabled investments and IT ensures optimisation of the costs of delivering IT capabilities and services.	3	Requirements are aligned to SLAs in SLM1		no

		ME4.4	**ME4.4 Resource Management** Oversee the investment, use and allocation of IT resources through regular assessments of IT initiatives and operations to ensure appropriate resourcing and alignment with current and future strategic objectives and business imperatives.	3	The databses used in ISM processes can provide relevant information to support this.		no
		ME4.5	**ME4.5 Risk Management** Work with the board to define the enterprise's appetite for IT risk, and obtain reasonable assurance that IT risk management practices are appropriate to ensure that the actual IT risk does not exceed the board's risk appetite. Embed risk management responsibilities into the organisation, ensuring that the business and IT regularly assess and report IT-related risks and their impact and that the enterprise's IT risk position is transparent to all stakeholders.	2	Fully covered in QM Organizational roles are covered in the Publishing Tool.	QM	no
		ME4.6	**ME4.6 Performance Measurement** Confirm that agreed-upon IT objectives have been met or exceeded, or that progress toward IT goals meets expectations. Where agreed-upon objectives have been missed or progress is not as expected, review management's remedial action. Report to the board relevant portfolios, programme and IT performance, supported by reports to enable senior management to review the enterprise's progress toward identified goals.	2	Service achievements are reported and discussed in the SLM2 process, based on reports from lower-level processes and functions. Remedial actions are covered in both the SLM process and the QM process.	SLM2, QM	no
		ME4.7	**ME4.7 Independent Assurance** Obtain independent assurance (internal or external) about the conformance of IT with relevant laws and regulations; the organisation's policies, standards and procedures; generally accepted practices; and the effective and efficient performance of IT.	3	The databses used in ISM processes can provide relevant information to support this.		no