



Security, Audit and Control Features SAP® R/3® 2nd Edition

Audit Programs and Internal Control Questionnaires

ISACA®

With more than 50,000 members in more than 140 countries, ISACA (www.isaca.org) is a recognized worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the *Information Systems Control Journal*®, develops international information systems auditing and control standards, and administers the globally respected Certified Information Systems Auditor™ (CISA®) designation earned by more than 48,000 professionals since inception, and Certified Information Security Manager® (CISM®) designation, a groundbreaking credential earned by 6,000 professionals since the program's inception.

Purpose of Audit Programs and Internal Control Questionnaires

One of ISACA's goals is to ensure that educational products support member and industry information needs. Responding to member requests for useful audit programs, ISACA's Education Board has released audit programs and internal control questionnaires, for member use through K-NET. These products are developed from ITGI publications, or provided by practitioners in the field.

Control Objectives for Information and related Technology

Control Objectives for Information and related Technology (COBIT®) has been developed as a generally applicable and accepted framework for good information technology (IT) security and control practices for management, users, and IS audit, control and security practitioners. The audit programs included in K-NET have been referenced to key COBIT control objectives.

Disclaimer

ISACA (the "Owner") has designed and created this publication, titled *Security, Audit and Control Features SAP® R/3®: A Technical and Risk Management Reference Guide, 2nd Edition* (the "Work"), primarily as an educational resource for control professionals. The Owner makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, the control professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

While all care has been taken in researching and documenting the techniques described in this text, persons employing these techniques must use their own knowledge and judgment. ISACA and Deloitte Touche Tohmatsu, its partners and employees, shall not be liable for any losses and/or damages (whether direct or indirect), costs, expenses or claims whatsoever arising out of the use of the techniques described, or reliance on the information in this reference guide.

SAP, SAP R/2, SAP R/3, mySAP, SAP R/3 Enterprise, SAP Strategic Enterprise Management (SAP SEM), SAP NetWeaver, ABAP, mySAP Business Suite, mySAP Customer Relationship Management, mySAP Supply Chain Management, mySAP Product Lifecycle Management, mySAP Supplier Relationship Management and other SAP product/services referenced herein are the trademarks or registered trademarks of SAP AG in Germany and in several other countries. The publisher gratefully acknowledges SAP's kind permission to use these trademarks in this publication. SAP AG is not the publisher of this book and is not responsible for it under any aspect of press law.

The purpose of these audit plans and internal control questionnaires (ICQs) is to provide the audit, control and security professional with a methodology for evaluating the subject matter of the ISACA publication *Security, Audit and Control Features SAP® R/3®: A Technical and Risk Management Guide*. They examine key issues and components that need to be considered for this topic. The review questions have been developed and reviewed with regard to COBIT 4.0. Note: The professional should customize the audit programs and ICQs to define each specific organization's constraints, policies and practices.

The following are included here:

- Revenue Business Cycle Audit Program Page 2
- Expenditure Business Cycle Audit Program Page 10
- Inventory Business Cycle Audit Program Page 19
- Basis Security Cycle Audit Program Page 24
- Revenue Business Cycle ICQ Page 43
- Expenditure Business Cycle ICQ Page 45
- Inventory Business Cycle ICQ Page 47
- Basis Security Cycle ICQ Page 51

Revenue Business Cycle Audit Program		
Control Objective/Test	Documentation/Matters Arising	COBIT Reference
A. Prior Audit/Examination Report Follow-up		
Review prior report, if one exists, verify completion of any agreed-upon corrections and note remaining deficiencies.		ME1
B. Preliminary Audit Steps		
Gain an understanding of the SAP R/3 environment.		
The same background information obtained for the SAP R/3 Basis Security audit plan is required for and relevant to the business cycles. In particular the following information is important: <ul style="list-style-type: none"> • Version and release of SAP R/3 that has been implemented • Total number of named users (for comparison with logical access security testing results) • Number of SAP instances and clients • Company codes • The identification of the modules being used (FI, CO, MM, SD, PP, industry-specific, etc.) • Whether the organization has created any locally developed ABAP programs or reports • Details of the risk assessment approach taken in the organization to identify and prioritize risks • Copies of the organization's key security policies and standards 		PO2 PO3 PO4 PO6 PO9 DS2 DS5 AI2 AI6 ME1 ME2
Obtain details of the following: <ul style="list-style-type: none"> • The Organizational Model as it relates to sales/revenue activity, i.e., sales organization unit structure in SAP R/3 and company sales organization chart (required when evaluating the results of access security control testing) • Interview systems implementation team if possible and obtain process design documentation for sales and distribution 		DS5 AI1 DS6

Revenue Business Cycle Audit Program		
Control Objective/Test	Documentation/Matters Arising	COBIT Reference
Identify the significant risks and determine the key controls.		
Develop a high-level process flow diagram and overall understanding of the revenue processing cycle including the following subprocesses: <ul style="list-style-type: none"> • Customer, material and pricing master data maintenance • Sales order processing • Shipping, invoicing, returns and adjustments • Collecting and processing cash receipts 		AI1 PO9 DS13
Assess the key risks, determine key controls or control weaknesses and test controls (refer sample testing program below and chapter 4 for techniques for testing configurable controls and logical access security) regarding the following factors: <ul style="list-style-type: none"> • The controls culture of the organization (e.g., a just-enough-control philosophy). • The need to exercise judgement to determine the key controls in the process and whether the controls structure is adequate (Any weaknesses in the control structure should be reported to executive management and resolved.) 		DS5 DS9 PO9 ME2
C. Detailed Audit Steps		
1. Master Data Maintenance		
1.1 Changes made to master data are valid, complete, accurate and timely.		
1.1.1 Determine whether the following reports of changes to master data have been compared to authorized source documents and/or a manual log of requested changes to ensure they were input accurately and timely: <ul style="list-style-type: none"> • For customer master data, transaction OV51 or the report RFDABL00 will generate a list denoting the date and time of change, old and new values for fields and details of the user who input the change. • Report RFDKLIAB—Display changes to Credit Management; can be run to display credit information change details for comparison to authorized source documents. • Transaction MM04 can be used to display master data changes for individual materials. • A list of pricing changes can be generated using transaction VK12 and subsequently selecting the menu-options <i>Environment, changes, report</i> (change documents). Check the accuracy of changes made to the pricing master records and also the timing at which these changes have been applied (which is essential to the effective processing of pricing changes) against authorized source documentation. 		DS11 AI2 AI6 DS6

Revenue Business Cycle Audit Program

Control Objective/Test	Documentation/Matters Arising	COBIT Reference
<p>1.1.2 Review organization policy and process design specifications regarding access to maintain master data. Test user access to create and maintain customer, material and pricing master data as follows:</p> <ul style="list-style-type: none"> • Customer Master Data—transaction codes FD02 (Finance), VD02 (Sales), XD02 (Central) • Material Master Data—transaction codes MM01 (Create), MM02 (Change). • Pricing Master Data—transaction codes VK11 and VK12 • Credit Limit—Transaction codes FD24 and FD32 • Codes—Create (01), block (05) and delete (06) 		<p>DS5 AI2 AI6 DS11</p>
<p>1.1.3 Determine whether the configurable control settings address the risks pertaining to the validity, completeness and accuracy of master data and whether they have been set in accordance with management intentions. View the settings online using the IMG as follows:</p> <ul style="list-style-type: none"> • Customer Account Groups: Transaction SPRO Menu Path—Financial Accounting> Accounts Receivable Accounts Payable> Customer Accounts> Master Records> Preparation for Creating Customer Master Records> Define account group with screen layout. • Material Types: Transaction SPRO Menu Path—Logistics General> Material Master> Basic Settings> Material Types> Define attributes of material types. • Industry Sector: Transaction SPRO Menu Path—Logistics General> Material Master> Field Selection> Define industry sectors and industry-sector-specific field selection • Understand the organization’s pricing policy and its configuration in SAP R/3 (e.g., hard-coded, manual over-ride possible, user enters price). Pricing condition types and records can be reviewed against the organization’s pricing policy using the following menu path and transaction codes: <ul style="list-style-type: none"> - Transaction SPRO Menu Path—Sales and Distribution> Basic Functions> Pricing - V-44 for material price condition record - V-48 price list type condition records - V-52 Customer specific condition type 		<p>DS9 DS12 DS11 PO9</p>

Revenue Business Cycle Audit Program

Control Objective/Test	Documentation/Matters Arising	COBIT Reference
1.2 Master data remain current and pertinent.		
1.2.1 Determine whether management runs the following reports, or equivalent, by master data type and confirm evidence of their review of the data for currency and ongoing pertinence: <ul style="list-style-type: none"> • Customer Master Data: Run report RFDKVZ00. • Material master Data: Run report RMMVRZ00. • Pricing Master Data: Run transaction VK13. <p>Transaction F.32 provides an overview of customers for which no credit limit has been entered. Check the output from Transaction F.32 to confirm a credit limit has been set for customers in the range requiring a limit.</p>		DS3 PO8 ME1 DS11
1.2.2 Determine whether appropriate credit limits have been loaded for customers.		
2.1 Sales orders are processed with valid prices and terms and processing is complete, accurate and timely.		
2.1.1 Determine whether the ability to create, change or delete sales orders, contracts, and delivery schedules is restricted to authorized personnel by testing access to the following transactions: <ul style="list-style-type: none"> • Create/Change Sales Order VA01/VA02 • Create/Change Delivery Schedule VA31/VA32 • Create/Change Contracts VA41/VA42 		
2.1.2 Refer Master Data Integrity point 1.1.2.		
2.1.3 Refer Master Data Integrity point 1.1.3.		
2.1.4 Understand the policies and procedures regarding reconciliation of sales orders. Review operations activity at selected times and check for evidence that reconciliations are being performed.		
2.2 Orders are processed within approved customer credit limits.		

Revenue Business Cycle Audit Program

Control Objective/Test	Documentation/Matters Arising	COBIT Reference
<p>2.2.1 Determine whether the configurable control settings address the risks pertaining to the processing of orders outside customer credit limits and whether they have been set in accordance with management intentions. View the settings online using the IMG as follows:</p> <ul style="list-style-type: none"> • Transaction SPRO Menu Path: Financial Accounting> Accounts Receivable Accounts Payable> Credit Management> Credit Control Account • Execute transaction OVAK to show the type of credit check performed for the corresponding transaction types in order processing. • Execute transaction OVA7 to determine whether a credit check is performed for appropriate document types being used. • Execute transaction OVAD to show the credit groups that have been assigned to the delivery types being used. • Execute transaction OVA8 to show an overview of defined credit checks for credit control areas. 		
<p>2.3 Order entry data are completely and accurately transferred to the shipping and invoicing activities.</p>		
<p>2.3.1 A full list of incomplete sales documents can be obtained from the system using Transaction V.00—List Incomplete SD Documents or through the transaction RVAUFERR. Review items on the list with the appropriate operational management and ascertain if there are legitimate reasons for the sales documents that remain incomplete.</p>		
<p>3. Shipping, Invoicing, Returns and Adjustments</p>		
<p>3.1 Controls are in place to prevent duplicate shipments or delay in the shipping of goods to customers.</p>		
<p>3.1.1 Generate the list of current system configuration settings relating to copy control between sales and shipping documents using Transaction: VTLA—Display Copying Control: Sales Document to Delivery Document. Select each combination of delivery type and sales document type and click the Item button. Double click on each item category and verify that the entry for the indicator Qty/value pos./neg. has been set to + (automatic update occurs between documents as deliveries are made for line items specified in the sales document).</p>		

Revenue Business Cycle Audit Program

Control Objective/Test	Documentation/Matters Arising	COBIT Reference
<p>3.1.2 Determine whether the following shipping reports are used to assist in controlling the shipping process:</p> <ul style="list-style-type: none"> • Backlog Reports—V.15 • Process Delivery Due List – VL04 or transaction RV50SBT1 • Outbound Deliveries for Picking—VL06 • Outbound Deliveries for Confirmation—VL06C • Outbound Deliveries to be Loaded—VL06L • Deliveries for Transportation Planning—VL06T • Deliveries for Goods Issue List—VL06G <p>Interview management and determine whether any of the above reports are used to check the complete and timely shipment of goods to customers. Review a sample of any hardcopy reports used for evidence of action taken and/or review a sample of the reports online and check the aging of items to determine if entries have been cleared in a timely manner.</p>		
<p>3.2 Invoices are generated using authorized terms and prices and are accurately calculated and recorded.</p>		
<p>3.2.1 Display current system settings relating to invoice preparation online using the IMG:</p> <ul style="list-style-type: none"> • Transaction SPRO Menu Path—Sales and Distribution> Billing> Billing Documents. <p>Determine whether the connection between source and target documents supports the accurate flow of billing details through the sales process and supports the accurate calculation and posting of invoice data.</p>		
<p>3.3 All goods shipped are invoiced and invoiced in a timely manner.</p>		
<p>3.3.1 Execute transaction VF04—Process Billing Due List. All documents that have not been invoiced, or that have been only partially invoiced, will appear on the list, sorted by invoice due date. Review the aging of items in the list. For items outstanding for more than one billing period, seek an explanation from management as to why the items have not been billed.</p>		
<p>3.3.2 Assess user access to picking lists, delivery notes and goods issues by testing access to the following transactions:</p> <ul style="list-style-type: none"> • Create Single Delivery—VL01 • Create Multiple Deliveries—VL04 • Change Deliveries—VL02 		

Revenue Business Cycle Audit Program

Control Objective/Test	Documentation/Matters Arising	COBIT Reference
<p>3.3.3 Execute transaction VF03 Display Invoice and click on the expansion button next to the billing document field and select Billing Documents Still to Be Passed Onto Accounting. Obtain explanation for any invoices that appear in this list. Test user access to transactions to enter invoices and confirm this is consistent with staff job roles and management’s intentions.</p> <ul style="list-style-type: none"> • Sales Accounts Receivable Entry—VF01 and VF04 • Finance Entry—FB70 		
<p>3.4 Credit notes and adjustments to accounts receivable are accurately calculated and recorded.</p>		
<p>3.4.1 Assess user access to sales order return and credit notes transactions as follows:</p> <ul style="list-style-type: none"> • Sales entry: Create Sales Document—VA01 • Sales entry: Change Sales Document—VA02 • Finance Entry—FB75 		
<p>3.5 Credit notes for all goods returned and adjustments to accounts receivable are issued in accordance with organization policy and issued in a timely manner.</p>		
<p>3.5.1 View the sales document types configured by using transaction VOV8. Look for the entire sales document types that relate to sales order returns and credit requests. Double click on one of these document types. In the General Control section of the screen, there is a Reference mandatory field. Verify that the setting has been set to M. Repeat this for all of the other relevant document types. Discuss the Reference field settings in place for the selected document types with management. Determine whether the configuration in place is set as management intended.</p>		
<p>3.5.2 Review the configuration settings for delivery and billing blocks online using the IMG as follows:</p> <ul style="list-style-type: none"> • Shipping: Transaction SPRO Menu Path: Logistics Execution> Shipping> Deliveries> Define Reasons for Blocking in Shipping • Billing: Transaction SPRO Manu Path: Sales and Distribution> Billing> Billing Documents> Define Blocking Reason for Billing <p>Determine whether the settings support the processing of credits in line with the organization’s credit management policy and are consistent with management’s intention.</p>		
<p>4. Collecting and Processing Cash Receipts</p>		
<p>4.1 Cash receipts are entered accurately, completely and in a timely manner.</p>		
<p>4.1.1. Take a sample of bank reconciliations and test for adequate clearance of reconciling items and approval by finance management.</p>		

Revenue Business Cycle Audit Program

Control Objective/Test	Documentation/Matters Arising	COBIT Reference
4.1.2 Determine whether the system has been configured to not allow processing of cash receipts outside of approved bank accounts. Execute transaction FI12 and ascertain to which bank accounts a cash receipt can be posted. Determine if this is consistent with management's intentions.		
4.1.3 Use transaction SA38 to produce the following reports: <ul style="list-style-type: none"> • The Customer Open Items report (RFDOPO00) • The Customer Open Item Analysis (days overdue analysis) report (RFDOPR10) Determine whether these reports are reviewed and actioned regularly by locating evidence of their review or through corroborative inquiry with management.		
4.2 Cash receipts are valid and are not duplicated.		
4.2.1 Review the accounts receivable reconciliation and determine whether there are any amounts unallocated or any reconciling items. Determine the aging of these items and make inquiry of management as to the reasons for these items remaining unallocated or unreconciled.		
4.3 Cash discounts are calculated and recorded accurately.		
4.3.1 Review the settings in place for tolerance levels for allowable cash discounts and cash payment differences by the following transactions: <ul style="list-style-type: none"> • OBA4, to determine the tolerance groups that have been set up for users and the tolerance limits that have been set for those groups • OB57, to determine the users who have been allocated to the groups identified earlier Discuss with management the settings that are in place for tolerance levels for allowable cash discounts and cash payment differences. Determine whether the configuration in place agrees with management's intentions.		
4.4 Timely collection of cash receipts is monitored.		
4.4.1 As for 4.1.3, determine whether accounts receivable aging reports are reviewed regularly to ensure that the collection of payments is being performed in a timely manner.		

Expenditure Business Cycle Audit Program		
Control Objective/Test	Documentation/Matters Arising	COBIT Reference
A. Prior Audit/Examination Report Follow-up		
Review prior report, if one exists, verify completion of any agreed upon corrections, and note remaining deficiencies.		ME1
B. Preliminary Audit Steps		
Gain an understanding of the SAP R/3 environment.		
The same background information obtained for the SAP R/3 Basis Security audit plan is required for and relevant to the business cycles. In particular the following information is important: <ul style="list-style-type: none"> • The version and release of SAP R/3 implemented • Total number of named users (for comparison with logical access security testing results) • Number of SAP instances and clients • Company codes • The identification of the modules being used (FI, CO, MM, SD, PP, industry-specific, etc.) • If the organization has created any locally developed ABAP programs or reports • Details of the risk assessment approach taken in the organization to identify and prioritize risks • Copies of the organization's key security policies and standards 		PO2 PO3 PO4 PO6 PO9 DS2 DS5 AI2 AI6 ME2
Obtain details of the following: <ul style="list-style-type: none"> • The Organizational Model as it relates to expenditure activity, i.e., purchasing organization unit structure in SAP R/3 and purchasing/accounts payable organization chart (required when evaluating the results of access security control testing) • An interview of the systems implementation team, if possible, and the process design documentation for materials management 		DS5 AI1 PO7
Identify the significant risks and determine the key controls.		
Develop a high-level process flow diagram and overall understanding of the expenditure processing cycle including the following subprocesses: <ul style="list-style-type: none"> • Master data maintenance • Purchasing • Invoice processing • Processing disbursements 		PO9 AI1 DS11
Assess the key risks, determine key controls or control weaknesses and test controls (refer sample testing program below and chapter 4 for techniques for testing configurable controls and logical access security) regarding the following factors: <ul style="list-style-type: none"> • The controls culture of the organization (e.g., a just-enough control philosophy) • The need to exercise judgement to determine the key controls in the process and whether the controls structure is adequate (Any weaknesses in the control structure should be reported to executive management and resolved.) 		DS9 PO9 DS5 ME2

Expenditure Business Cycle Audit Program

Control Objective/Test	Documentation/Matters Arising	COBIT Reference
C. Detailed Audit Steps		
1. Master Data Maintenance		
1.1 Changes made to master data are valid, complete, accurate and timely.		
<p>1.1.1 Determine whether the changes made to the master data are complete, accurate, timely and using the specified transaction code or SA38, whether the following report of changes to master data are compared to authorized source documents and/or a manual log of requested changes to ensure they were input accurately and timely.</p> <ul style="list-style-type: none"> ● For vendor master data, the program RFKABL00 can be used to produce a list of master data changes. 		<p>AI6 DS11</p>
<p>1.1.2 Determine whether access to create and change vendor pricing master data is restricted to a dedicated area and to authorized individuals. Review organization policy and process design specifications regarding access to maintain master data. Test user access via report RSUSR002 (refer to chapter IV on how to test user access) to create and maintain vendor master data as follows:</p> <ul style="list-style-type: none"> ● Finance Entry—transaction codes FK01 (Create), FK02 (Change), FK05 (Block/Unblock), FK06 (Delete) ● Purchasing Entry—transaction codes MK01 (Create), MK02 (Change), MK05 (Block/Unblock), MK06 (Delete) ● Centralized Entry—transaction codes XK01 (Create), XK02 (Change), XK05 (Block/Unblock), XK06 (Delete) <p>Test user access to transactions to maintain vendor pricing information:</p> <ul style="list-style-type: none"> ● Create info record—ME11 ● Change info record—ME12 ● Delete info record—ME15 ● Create condition—MEK1 ● Change condition—MEK2 ● Create condition with reference—MEK4 		<p>DS5 AI6 DS6 DS11</p>
<p>1.1.3 Determine whether the configurable control settings address the risks pertaining to the validity, completeness and accuracy of master data and whether they have been set in accordance with management intentions. View the settings online using the IMG as follows:</p> <ul style="list-style-type: none"> ● Execute transaction code OBD3 and ascertain whether account groups have been set up covering one-time vendor or other vendor accounts. For high-risk account groups such as one-time vendors, check whether authorization has been marked as a required field. 		<p>DS12 DS9 DS11</p>

Expenditure Business Cycle Audit Program

Control Objective/Test	Documentation/Matters Arising	COBIT Reference
1.1.4 Determine whether a naming convention should be used for vendor names (e.g., as per letterhead) to minimize the risk of establishing duplicated vendor master records. Extract a list of vendor account names from table LFA1 (Fields: NAME1=name, LIFNR= vendor number). Review a sample for compliance with the organization’s naming convention. View or search the list (using scan search software tools if available) for potential duplicates.		DS11 PO9
1.2 Master data remain current and pertinent.		
1.2.1 Determine whether management periodically reviews master data to check their currency and ongoing pertinence, and whether the appropriate management displays or produces a list of vendors using report RFKKVZ00 or equivalent. Confirm evidence of management’s review of the data on a rotating basis for currency and ongoing pertinence.		DS11 ME1
2. Purchasing		
2.1 Purchase order entry and changes are valid, complete, accurate and timely.		
2.1.1 Determine whether purchase orders are processed with valid process and terms and if processing is complete, accurate and timely. Determine whether the ability to create, change, or cancel purchase requisitions, purchase orders and outline agreements (standing purchase orders) is restricted to authorized personnel by testing access to the following transactions: <ul style="list-style-type: none"> • Create Purchase Requisition—ME51 • Change Purchase Requisition—ME52 • Release Purchase Requisition—ME54 • Collective Release of Purchase Requisition—ME55 • Create Purchase Order, Vendor known—ME21 • Change Purchase Order—ME22 • Maintain Purchase Order Supplement—ME24 • Create Purchase Order, Vendor unknown—ME25 • Creation of Stock Transport Order—ME27 • Create Outline Agreement—ME31 • Change Outline Agreement—ME32 • Maintain Outline Agreement Supplement—ME34 		DS11 DS5

Expenditure Business Cycle Audit Program

Control Objective/Test	Documentation/Matters Arising	COBIT Reference
<p>2.1.2 Determine whether the SAP R/3 source list functionality allows only specified materials to be purchased from vendors included in the source list for the specified material. Through discussions with management, determine (types of) materials for which source lists should be available in the system. Also, determine (types of) materials for which a source list should not be present. Examine a selection of materials and view the corresponding source list using the following reports to corroborate the performance of the control activity in the appropriate accounting period:</p> <ul style="list-style-type: none"> • ME06 reports on all material items and whether they belong to a source list or not • ME0M shows all material items and any associated vendors (including historic data). To run ME0M, a material or a range of materials needs to be specified. Use the matchcode and click on the search help option and choose option J—material by material group—to get a list of materials. <p>Select the above-mentioned sample of orders and check against source list reports to determine if specific materials have been procured with unlisted vendors.</p>		DS11

Expenditure Business Cycle Audit Program

Control Objective/Test	Documentation/Matters Arising	COBIT Reference
<p>2.1.3 Determine whether the SAP R/3 release strategy is used to authorize purchase orders, outline agreements (standing purchase orders) and unusual purchases (e.g., capital outlays). Obtain sufficient understanding of the system configuration to assess the adequacy of the release strategy as defined and implemented by the organization, as well as the function and effectiveness of established policies, procedures, standards, and guidance. The following transactions should be executed to obtain an understanding of the way the system has been configured:</p> <ul style="list-style-type: none"> • Release procedure: Purchase Orders—OMGS and release procedure Purchase Requisitions (with classification)—OMGQ <ul style="list-style-type: none"> - Click on Release Strategy. Select the strategies one by one, by double-clicking on the strategy. Note the release codes that are shown—authorization (authorization objects M_BANF_FRG and M_EINK_FRG) for these release codes should be checked. - Click on Classification. This will show the conditions under which the purchase document will be blocked. Ascertain if these conditions comply with management’s intentions. • Release procedure Purchase Requisitions (without classification)—OME6 <ul style="list-style-type: none"> - Click on Release Prerequisites. Note the release codes that are shown - authorization for these release codes should be checked. - Re-execute transaction OME6 and click on Determination of Release Strategy. This will show the conditions under which the purchase document will be blocked. Ascertain if these conditions comply with management’s intentions. • Test user access to transactions for release strategies: <ul style="list-style-type: none"> - Release Purchase Order—ME28 - Release Outline Agreement—ME35 - Release Purchase Requisition—ME54 - Collective Release of Purchase Requisitions—ME55 		<p>DS9 DS5 ME1 DS13</p>
<p>2.2 Goods are only received for valid purchase orders and goods receipts are recorded completely, accurately and in a timely manner.</p>		

Expenditure Business Cycle Audit Program

Control Objective/Test	Documentation/Matters Arising	COBIT Reference
<p>2.2.1 Determine whether goods (or materials, equipment) are received only when there are valid purchase orders, or if goods receipts are always recorded completely, accurately and in a timely manner. Determine whether an investigation takes place when receipts have no purchase order or exceed the purchase order quantity by more than an established amount. Does management review exception reports of goods not received on time for recorded purchases? Run the report RM06EM00 to produce a listing of Purchase Orders Outstanding. Ascertain from management if there are any reasons for any long outstanding items on the report.</p>		<p>DS9 DS5</p>
<p>2.2.2 Determine whether order entry data are transferred completely and accurately to the shipping and invoicing activities, and if the ability to input, change or cancel goods received transactions is restricted to authorized inbound logistics/raw materials personnel. Test user access to transactions for goods receipt as follows:</p> <ul style="list-style-type: none"> • Goods Receipt for Purchase Order—MB01 • Goods Receipts, Purchase Order Unknown—MB0A • Goods Receipt for Production Order—MB31 • Other Goods Receipts—MB1C • Cancel/reverse Material Document—MBST <p>Test user access to high-risk movement types transaction code MB1C, authorization object M_MSEG_BWA and fields ACTV and movement types BWART 561 through 566. These special movement types reflect the initial stock entry in the SAP R/3 system at the time of conversion to the SAP R/3 system.</p>		<p>AI2 DS5 DS11</p>
<p>2.3 Defective goods are returned to suppliers in a timely manner.</p>		
<p>2.3.1 Determine whether defective goods (or materials, equipment) are returned in a timely manner to suppliers, are adequately segregated from other goods in a quality-assurance bonding area, and are regularly monitored (assigned a specific movement type, e.g., 122) to ensure timely return to suppliers and whether credit is received in a timely manner. Ascertain from management the movement type used to block processing and for returning rejected goods to suppliers (e.g., movement type 122). Execute transaction MB51 with the appropriate movement type. Determine if there are any long outstanding materials pending return to suppliers/receipt of appropriate credits.</p>		<p>DS2 DS11</p>
<p>3. Invoice Processing</p>		
<p>3.1 Amounts posted to accounts payable represent goods or services received.</p>		

Expenditure Business Cycle Audit Program

Control Objective/Test	Documentation/Matters Arising	COBIT Reference
<p>3.1.1 Determine whether amounts posted to accounts payable represent goods or services received, the ability to input, change, cancel or release vendor invoices for payment is restricted to authorized personnel and the ability to input vendor invoices that do not have a purchase order and/or goods receipt is restricted to authorized personnel. Test user access to transactions for invoice processing:</p> <ul style="list-style-type: none"> • Enter Invoice MRHR, MR01 • Change Invoice FB02 • Process Blocked Invoice MR02 • Cancel Invoice MR08 • Enter Credit Memo MRHG 		<p>DS6 DS9 AI6</p>
<p>3.2 Accounts payable amounts are calculated completely and accurately and recorded in a timely manner.</p>		
<p>3.2.1 Determine whether the SAP R/3 software is configured to perform a three-way match. Execute transaction code OMF4—(Change View “field Selection at document level”: Overview) by selecting ME21—(Create Purchase Order) and then selecting GR/IR Control. Determine whether GR/IR Control has been set globally to required entry. If the GR/IR Control indicator has not been set globally for all vendors, determine whether it has been set for particular vendors by displaying table LFM1, field name WEBRE, using transaction SE16. Where GR/IR Control has not been set, ascertain if there are any reasons from management.</p>		<p>DS9 DS5</p>
<p>3.2.2 Determine whether the SAP R/3 software is configured with quantity and price tolerance limits. Tolerance limits for price variances and message settings for invoice verification (online matching) should be checked as follows:</p> <ul style="list-style-type: none"> • Variance settings:— Execute transaction OMEU & OMR6. The system will now show an overview of the defined tolerance limits. Double-click on the entries that relate to the organization being audited. Two entries need to be checked, one for tolerance key PE (price) and one for tolerance key SE (discount). Note the values shown. Both a lower and upper limit may be specified as a percentage value. (PE also allows setting of an absolute value.) • Message settings: — Execute transaction OME0. Click on button Position. Enter values 00, 06 and 207 (message for price variance) and press Enter. Note the value in the categories field. Possible values are W for warning and ‘E’ for error. <p>Ascertain whether the values noted comply with management intentions.</p>		<p>DS9 DS10</p>

Expenditure Business Cycle Audit Program

Control Objective/Test	Documentation/Matters Arising	COBIT Reference
3.2.3 Determine whether the GR/IR account balances (RM07MSAL) report is executed and reviewed periodically. Check that there are appropriate procedures in place to investigate unmatched purchase orders. In particular, long outstanding items should be followed-up and cleared.		AI6
3.2.4 Determine whether reports of outstanding purchase orders are reviewed regularly. Run the report RM06EM00 to produce a listing of Purchase Orders Outstanding and review long outstanding items with management.		PO11
3.2.5 Determine whether the SAP R/3 software restricts the ability to modify the exchange- rate table to authorized personnel, management approves values in the centrally maintained exchange rate table and the SAP R/3 software automatically calculates foreign currency translations, based on values in the centrally maintained exchange rate table. Determine whether management reviews a sample of changes to exchange rates above a certain percentage having regard to the volume and value of foreign currency transactions for the organization. Test user access to the exchange rates and the related authorization objects: <ul style="list-style-type: none"> • Exchange rate via standard transaction First, execute transaction SUCU. Click on Position. Enter value V_TCURR and press Enter. Note the value in the field Authorization Group. Then test user access to transaction code OB08, Authorization Object: S_TABU_DIS (Class Basis: Administration), Field Activity: value 02 and Field Authorization Group: Value noted with transaction SUCU. • Exchange rate via view maintenance First, execute transaction SUCU. Click on Position. Enter Table Name value V_T001R, Click on Choose. Note the value in the field authorization group. Do the same for table V_TCURF. Then test user access to transaction codes as follows with Authorization Object: S_TABU_DIS (Class Basis: Administration), Field Activity: 02 and Field Authorization group: Value noted with transaction SUCU: <ul style="list-style-type: none"> - Maintain table rounding units—OB90 - Maintain table foreign currency ratios—OBBS - Table view maintenance—SM30. 		DS5 AI6
3.3 Credit notes and other adjustments are calculated completely and accurately and recorded in a timely manner.		
3.3.1 Determine whether the ability to input, change, cancel or release credit notes is restricted to authorized personnel. Test user access to post invoices directly to vendor accounts: <ul style="list-style-type: none"> • Enter Credit Note—F-41 • Enter Invoice—F-43 		PO2 DS5

Expenditure Business Cycle Audit Program

Control Objective/Test	Documentation/Matters Arising	COBIT Reference
4. Processing Disbursements		
4.1 Disbursements are made only for goods and services received, calculated accurately, recorded and distributed to the appropriate suppliers in a timely manner.		
4.1.1 Determine whether disbursements are made only for goods and services received, calculated accurately, recorded and distributed to the appropriate suppliers in a timely manner, and whether management approves the SAP R/3 payment run parameter specification. Test user access to transactions to process disbursements: <ul style="list-style-type: none"> • Automatic payment transactions—F110 • Parameters for payment —F111 • Payment with printout—F-58 		DS5 PO6
4.1.2 Test user access to blocked invoices : <ul style="list-style-type: none"> • Change document—FB02 • Change line items—FB09 • Block/unblock vendor (centrally)—XK05 • Block/unblock vendor—FK05 		

Inventory Business Cycle Audit Program		
Control Objective/Test	Documentation / Matters Arising	COBIT Reference
A. Prior Audit/Examination Report Follow-up		
Review prior report, if one exists, verify completion of any agreed upon corrections and note remaining deficiencies		ME1
B. Preliminary Audit Steps		
Gain an understanding of the SAP R/3 environment.		
<p>The same background information obtained for the SAP R/3 Basis Security audit plan is required for and relevant to the business cycles. In particular the following information is important:</p> <ul style="list-style-type: none"> • The version and release of SAP R/3 that has been implemented • Total number of named users (for comparison with logical access security testing results) • Number of SAP instances and clients • Company codes • The identification of the modules (FI, CO, MM, SD, PP, industry-specific, etc.) being used • Whether the organization has created any locally developed ABAP programs or reports • Details of the risk assessment approach taken in the organization to identify and prioritize risks • Copies of the organization's key security policies and standards • A review of outstanding audit findings, if any, from previous years 		PO2 PO3 PO4 PO6 PO9 DS2 DS5 AI2 AI6 ME2
<p>Obtain the following relevant business cycle details:</p> <ul style="list-style-type: none"> • The organizational model as it relates to inventory activity, i.e., plant organization unit structure in SAP R/3 and manufacturing organization chart (required when evaluating the results of access security control testing) • Interview systems implementation team if possible and obtain process design documentation for materials and warehouse management 		PO4 AI4
Identify the significant risks and determine the key controls.		
<p>Develop a high-level process flow diagram and overall understanding of the inventory processing cycle including the following subprocesses:</p> <ul style="list-style-type: none"> • Master data maintenance • Raw materials management • Producing and costing inventory • Handling and shipping finished goods 		DS11 DS12 DS6 DS13

Inventory Business Cycle Audit Program

Control Objective/Test	Documentation / Matters Arising	COBIT Reference
<p>Assess the key risks, determine key controls or control weaknesses and test controls (refer detailed sample testing program below and chapter 4 for techniques for testing configurable controls and logical access security) having regard to the following factors:</p> <ul style="list-style-type: none"> • The controls culture of the organization (e.g., a just-enough control philosophy) • The need to exercise judgement to determine the key controls in the process and whether the controls structure is adequate (Any weaknesses in the control structure should be reported to executive management and resolved.) 		PO9 ME2
C. Detailed Audit Steps		
1. Master Data Maintenance		
<i>Changes made to master data are valid, complete, accurate and timely</i>		
<p>1.1.1 Take a sample of inventory file updates using transaction MB59, which allows users to perform a search on multiple materials by a particular range of dates and check back to authorized source documentation. Review the process for physical stock-takes to confirm the complete, accurate, valid and timely recording of stock differences.</p>		DS11 DS13
<p>1.1.2 Review organization policy and process design specifications regarding access to maintain material master data. Test user access to the following transaction codes:</p> <ul style="list-style-type: none"> • Create Material—MM01 • Change Material—MM02 • Flag Material for Deletion—MM06 		DS11 DS13

Inventory Business Cycle Audit Program

Control Objective/Test	Documentation / Matters Arising	COBIT Reference
<p>1.1.3 Determine whether the configurable control settings address the risks pertaining to the validity, completeness and accuracy of master data and whether they have been set in accordance with management intentions. View the settings online using the IMG as follows:</p> <ul style="list-style-type: none"> • Material Types: Transaction SPRO Menu Path—Logistics General> Material Master> Basic Settings> Material Types> Define Attributes of Material Types • Industry Sector: Transaction SPRO Menu Path—Logistics General> Material Master> Field Selection> Define industry sectors and industry-sector-specific field selection • Default Price Types: Execute transaction OMW1 and determine whether default settings have been set for the price type for material records • Tolerances for Physical Inventory differences: Execute transaction OMJ2 and compare defined tolerances to organizational policy and judge for reasonableness 		PO9 DS11 DS12 DS13 DS6 ME1 ME2
1.2 Inventory master data remain current and pertinent.		
<p>1.2.1 Determine whether the appropriate management run the Materials List transaction code MM60, or equivalent by material type and confirm evidence of their review of the data on a rotating basis for currency and ongoing pertinence.</p>		ME1 DS11 ME4
1.3 Settings or changes to the bill of materials or process order settlement rules are valid, complete, accurate and timely.		
<p>1.3.1 Review organization policy and process design specifications regarding access to maintain bill of materials (BOM) and process order settlement rules. Test user access to the following transaction codes:</p> <ul style="list-style-type: none"> • Create Material BOM—CS0 • Change Material BOM—CS02 • Make Mass Changes—CS20 • Change Single-layered BOM—CS72 • Change Multi-layered BOM—CS75 • Change Settlement Rules—nondisplayable transaction code KOBK (refer to menu path: Logistics > Production Process > Process Order > Process Order > Display > Enter the process order number and press Enter then go to Header > Settlement Rule) 		ME1 DS13
<p>1.3.2 Take a sample of bill of materials updates using transaction CS80 and check back to authorized source documentation.</p>		DS13
2. Raw Materials Management		
2.1 Inventory is saleable, useable and safeguarded adequately.		

Inventory Business Cycle Audit Program

Control Objective/Test	Documentation / Matters Arising	COBIT Reference
2.1.1 Confirm that the DRP process takes into account stock on hand, forecast requirements, economic order quantities and back orders. Execute transaction code MB5M and ascertain the reason for any old stock being held (Shelf Life List). Use transaction MC46 to identify slow moving items and MC50 for “dead” stock (i.e., stock that has not been used for a certain period of time). Test that managers are reviewing this information on a regular basis.		DS6 DS13 ME1
2.2 Raw materials are only received and accepted with valid purchase orders and recorded accurately and in a timely manner.		
2.2.1 Test that management executes the report of outstanding purchase orders using transaction ME2L (refer Expenditure Cycle 2.2.1) and follow-up on any long outstanding items.		DS13
2.2.2 Review the reconciliation of the goods received/invoice received account (transaction code MB5S, refer Expenditure cycle 3.2.3) and confirm that unmatched items have been investigated in a timely manner.		ME1 ME2
2.2.3 Test user access to transactions for goods receipt (refer to the Expenditure cycle 2.2.2) as follows: <ul style="list-style-type: none"> • Goods Receipt for Purchase Order—MB01. • Goods Receipts Purchase Order Unknown—MB0A • Goods Receipt for Order—MB31 • Enter Other Goods Receipts—MB1C • Cancel Material Document—MBST • Goods Movement—MIGO 		DS13 ME1 DS12
2.2.4 Test the controls over inventory stock takes (refer 1.1.1).		
2.3 Defective raw materials are returned to suppliers in a timely manner.		
2.3.1 Ascertain from management the movement type used to block processing and for returning rejected goods to suppliers (e.g., movement type 122). Execute transaction MB51 with the appropriate movement type (refer Expenditure cycle 2.3.1). Determine if there are any long outstanding materials pending return to suppliers/receipt of appropriate credits.		DS13
3. Producing and Costing Inventory		
3.1 Transfers of materials to/from production, production costs and defective products/scrap are valid and recorded accurately, completely and in the appropriate period.		
3.1.1 Review the policy and procedures concerning the transfer of materials and confirm that the above controls are in place and operating. Test that inventory-in-transit accounts are regularly reviewed to ensure the accounts are cleared and reconciled. Confirm that default price types have been established for all materials (refer 1.1.3).		ME2 DS6
3.1.2 Test user access to bills of material (refer 1.3.1).		

Inventory Business Cycle Audit Program		
Control Objective/Test	Documentation / Matters Arising	COBIT Reference
3.1.3 Test user access to issue goods (transaction code MB1A), to posting of transfers between plants (transaction code MB1B) and to move goods (transaction code MIGO).		DS13 ME1
3.1.4 Test user access to create (transaction code CR01) or change (transaction code CR02) work centers.		DS13 ME1
4. Handling and Shipping Finished Goods		
4.1 Finished goods received from production are recorded completely and accurately in the appropriate period.		
4.1.1 Test inventory stock take procedures (refer 1.1.1)		DS13 ME1
4.1.2 Test user access to change settlement rules (refer 1.3.1).		ME1 DS13
4.2 Goods returned by customers are accepted in accordance with the organization's policies.		
4.2.1 Review the policies and procedures for receiving inventory back into the warehouse. Review some returns of inventory and ensure they are supported with adequate documentation from the quality inspector. Ascertain from management the movement type used for goods returned from customers. Execute transaction MB51 with the appropriate movement type. Determine if there are any long outstanding materials pending return to inventory/provision of appropriate credits.		ME1 AI4
4.3 Shipments are recorded accurately, in a timely manner and in the appropriate period.		
4.3.1 Test user access to transfer stock between plants (transaction code LT04) or Change Outbound Delivery (transaction code VL02N).		DS13 ME1
4.3.2 Take a sample of Deliver Due List and Owed to Customer Report and test for evidence of management action. Review settings using transaction code OMWB and confirm that accounts assignments are set to valid COGS accounts.		ME1 ME4 DS13

Basis Security Cycle Audit Program		
Control Objective/Test	Documentation / Matters Arising	COBIT Reference
A. Prior Audit/Examination Report Follow-up		
Review prior report, if one exists verify completion of any agreed upon corrections and note remaining deficiencies.		ME1
B. Preliminary Audit Steps		
Gain an understanding of the SAP R/3 environment.		
Determine what version and release of the SAP R/3 software has been implemented. If multiple versions, document the various versions.		PO4
Obtain details of the following: <ul style="list-style-type: none"> • Operating system(s) and platforms • Total number of named users (for comparison with limits specified in contract) • Number of SAP R/3 instances and clients • Database management system used to store data for the SAP R/3 system • Location of the servers and the related LAN/WAN connections (need to verify security and controls, including environmental, surrounding the hardware and the network security controls surrounding the connectivity) and, if possible, obtain copies of network topology diagrams • List of business partners, related organizations, and remote locations that are permitted to connect to the R/3 environment • Various means used to connect to the R/3 environment (e.g., dial-up, remote access server, Internet transaction server) and the network diagram if available 		PO2 PO3 DS2 DS12
In a standard SAP R/3 configuration, separate systems for development, test and production are implemented. Determine whether: <ul style="list-style-type: none"> • This approach was taken • The instances are totally separate systems or are within the same system 		PO2
Determine whether the SAP production environment is connected to other SAP or non-SAP systems. If yes, obtain details as to the nature of connectivity, frequency of information transfers, and security and control measures surrounding these transfers (i.e., to ensure accuracy and completeness).		PO2 DS5
Identify the modules (FI, CO, MM, SD, PP, industry-specific, etc.) that are being used.		PO2

Basis Security Cycle Audit Program

Control Objective/Test	Documentation / Matters Arising	COBIT Reference
Identify whether the organization has implemented any of the following: <ul style="list-style-type: none"> • Internet transaction server • Any of the New Dimension products (e.g., Supply Chain Management, Customer Relationship Management, Business Intelligence) • Audit information system. If implemented, determine how it is used (i.e., only for annual audits or on a regular basis to monitor and report on security issues). 		PO2 PO3 ME2
Determine whether the organization makes use of any mySAP.com functionality. If yes, describe functionality and purpose.		PO2
Determine whether the organization has created any locally developed APAB/4 programs/reports or tables. If yes, determine how these programs/reports are used. Depending on the importance/extent of use, review and document the development and change management process surrounding the creation/modification of these programs/reports or tables.		AI2 AI6
Obtain copies of the organization's key security policies and standards. Highlight key areas of concern, including: <ul style="list-style-type: none"> • Information security policy • Sensitivity classification • Logical and physical access control requirements • Network security requirements, including requirements for encryption, firewalls, etc. • Platform security requirements (e.g., configuration requirements) 		PO6 DS5 DS12
Obtain information regarding any awareness programs that have been delivered to staff on the key security policies and standards. Consider specifically the frequency of delivery and any statistics on the extent of coverage (i.e., what percentage of staff have received the awareness training).		PO6 DS7
Maintain authorizations and profiles, for example: <ul style="list-style-type: none"> • Have job roles, including the related transactions, been defined and documented? • Do procedures for maintaining (creating/changing/deleting) roles exist and are they followed? 		PO7 AI4 DS5

Basis Security Cycle Audit Program

Control Objective/Test	Documentation / Matters Arising	COBIT Reference
<p>Determine whether adequate access administration procedures exist in written form. Do any of the following procedures exist within the organization? (If yes, document the process and comment on compliance with the policies and standards, and the adequacy of resulting documentation.)</p> <ul style="list-style-type: none"> • Procedures to add/change/delete user master records • Procedures to handle temporary access requests • Procedures to handle emergency access requests • Procedures to remove users who have never logged into the system • Procedures to automatically notify the administration staff when staff holding sensitive or critical positions leave the organization or change positions 		PO7 AI4 DS5
<p>Obtain copies of the organization's change management policies, processes, procedures, and change documentation. Consider specifically:</p> <ul style="list-style-type: none"> • Transport processes and procedures, including allowed transport paths • Emergency change processes and procedures • Development standards, including naming conventions, testing requirements, and move-to-production requirements 		AI4 AI6
<p>Determine whether the organization has a defined process for creating and maintaining clients. If yes, obtain copies and documentation related to the creation and maintenance of clients.</p>		PO2 AI6
<p>Determine the organization's approach to SAP Online Support Services (OSS). Verify the extent of access permitted and processes used to request, approve, authenticate, grant, monitor, and terminate OSS access.</p>		DS2 DS5
<p>Review outstanding audit findings, if any, from previous years. Assess impact on current audit.</p>		ME1 ME2
<p>Identify the significant risks and determine the key controls.</p>		
<p>Obtain details of the risk assessment approach taken in the organization to identify and prioritize risks.</p>		PO9
<p>Obtain copies of and review:</p> <ul style="list-style-type: none"> • Completed risk assessments impacting the R/3 environment. • Approved requests to deviate from security policies and standards. <p>Assess the impact of the above documents on the planning of the R/3 audit.</p>		PO9 ME1
<p>In the case of a recent implementation/upgrade, obtain a copy of the security implementation plan. Assess whether the plan took into account the protection of critical objects within the organization and segregation of duties. Determine whether an appropriate naming convention (i.e., for profiles) has been developed to help security maintenance and to comply with required SAP R/3 naming conventions.</p>		PO3 DS5 PO7

Basis Security Cycle Audit Program		
Control Objective/Test	Documentation / Matters Arising	COBIT Reference
C. Detailed Audit Steps		
1. Application Installation (Implementation Guide and Organizational Model)		
1.1 Configuration changes are made in the development environment and transported to production.		
1.1.1 Test that access to the transaction code (SPRO) and the authorization object (S_IMG_ACTV) for the IMG has been restricted in the production environment.		
1.1.4 Restrict access to transaction code SCC4, which controls the production client settings. Execute this transaction code and then double click on each client being tested. Each of the settings should be reviewed for appropriateness. It is important to note that the No Changes setting should be set for cross-client tables. Also ensure that eCAAT and CAAT are set to Not Allowed.		
1.2 The Organizational Model has been configured correctly to meet the needs of the organization.		
1.2.1 Obtain information on the Organizational Model from the system by reviewing tables or by utilizing the SAP R/3 Audit Information System (AIS) that depicts the OM graphically (refer to figure 12.5). Compare it to the real organization structure and management interviewed in relation to differences or difficulties that may have emerged during or after the implementation.		
1.2.2 Test access to the transaction code (SPRO) and the authorization object (S_IMG_ACTV) for the IMG in the production environment.		
1.3 Changes to critical number ranges are controlled.		
1.3.1 Via transaction SUIM, review authorization object S_NUMBER (*) for those users with the following authorization value sets: <ul style="list-style-type: none"> • Maintain Number Range Intervals (02) • Change Number Range Status (11) • Initialize Number Levels (13) • Maintain Number Range Objects (17) for all Number Range Objects. 		
1.4 Access to system and customizing tables is restricted narrowly.		
1.4.1 By using transaction code SE16, browse table TDDAT. In the table name field enter Z* and then Y* to identify all of the custom tables. Determine those tables that have &NC& within the Authorization Group field. Assess whether these settings (&NC&) are appropriate.		
1.4.2 Access to modify critical tables can be tested via the objects S_TABU_DIS (value 02) and transaction codes SM31 or SM30. If the table is cross-client, the user master record must contain a third object, S_TABU_CLI (value X). Use RSUSR002 via SA38 to check for these restrictions.		

Basis Security Cycle Audit Program

Control Objective/Test	Documentation / Matters Arising	COBIT Reference
2. Application Development (ABAP/4 Workbench and Transport System)		
2.1 Application modifications are planned, tested and implemented in a phased manner.		
<p>2.1.1 Determine the system landscape and client strategy, and review the change control policies and procedures (including documentation) to transport objects between environments. Work with the Basis/Transport Administrator to obtain a random sample of transports and trace back to documentation. Ensure authorization for the transport was obtained and confirm that the specified transport path was followed. For emergency changes, ensure that the specified emergency process was followed. Confirm that appropriate authorizations were obtained and that documentation was subsequently completed.</p> <p>Review the system change option and confirm it has been set to No Changes Allowed (refer to 1.1.2 above). Review segregation of duties with respect to creating and releasing change requests. Test user access to authorization object S_TRANSPRT and ACTVT expect 03 and any Transport Type TTYPE. Assess the appropriateness of such access in comparison with the users' job functions.</p>		<p>A16 DS5</p>
2.2 Customized ABAP/4 programs are secured appropriately.		
<p>2.2.1 To identify customized programs that have not been assigned to an authorization group enter transaction code SE16. Browse the table TRDIR and enter the values of Z* and then Y* in the program name field. This will produce a list of all customized programs assuming that the organization has followed standard naming convention when customizing programs. Filter this list for programs that do not have a value in the authorization group field (SECU). Auditors should concentrate their investigations on users who have SE38, SA38, SE80 and SE37. These users will automatically have access to run many of these programs.</p>		
<p>2.2.2 From this list select a representative sample of customized programs and check the source code to see whether an Authority-Check statement has been included. Use transaction code SA38 and run the ABAP/4 program RSABAPSC with the appropriate program name and Authority-Check in the ABAP/4 language commands selection field to display the authority-check statements for each of the sampled programs. Note that the results may include other programs called by the sampled programs with the appropriate authority-check statements. The results of the test should be confirmed with management.</p>		

Basis Security Cycle Audit Program

Control Objective/Test	Documentation / Matters Arising	COBIT Reference
2.2.3 Review and assess the value for the parameters below (use RSPARAM report): <ul style="list-style-type: none"> • Auth/no_check_in_some_cases (Can be either Y or N. If set to the recommended value of Y (permit authorization checks), monitor the content of SU24 carefully to make sure that these entries are set appropriately) • Auth/rfc_authority_check (recommend set to 2 to permit full checking) 		DS5
2.2.4 Use report RSUSR002 to test the number of users who have access to execute all programs independent of the authorization group assigned. Enter the authorization object S_PROGRAM with the activity value of SUBMIT or BTCSUBMIT and the authorization object S_TCODE with a transaction code of SA38,SE37, SE38 or SE80		
2.2.5 Review the policy, procedures and criteria for establishing program authorization groups, assigning the ABAP/4 programs to groups and including authority-check statements in programs. Compare the results from testing to established policies, procedures, standards and guidance (note that organizations may use additional transactions, tables, authorization objects, ABAP/4 programs, and reports to control their systems).		
2.3 The creation or modification of programs is performed in the development system and migrated through the test system to production.		
2.3.1 Produce a list of users who have access to develop programs in the production system by executing report RSUSR002 with the authorization object S_DEVELOP, the activity values of 01, 02 or 06 and with the transaction code value SE38. ABAP/4 programs that are not assigned to an authorization group may be changed by any user with authorization for object S_DEVELOP, depending on whether the user has been assigned a developers key and the correct object keys.		
2.4 Access for making changes to the dictionary is restricted to authorized individuals.		
2.4.1 Execute the report RSUSR002. Review users with the following authorization to determine whether they are appropriate: <ul style="list-style-type: none"> • Data Dictionary object: S_DEVELOP with any of the Activity values 01, 02, 06, 07 and access to any of the transaction codes SE11, SE12, SE15, SE16, SE37, SE38, SE80 		

Basis Security Cycle Audit Program

Control Objective/Test	Documentation / Matters Arising	COBIT Reference
2.5 Access to modify and develop queries is restricted.		
2.5.1 Using report RSUSR002, enter the authorization object S_QUERY with activity value 02 and transaction code SQ01, to identify all users who can create and maintain queries. In addition, using the authorization object S_QUERY with activity value 23 and transaction codes SQ02 or SQ03, produce a report identifying all users who can maintain functional areas and user groups. Review the lists with management for reasonableness.		
2.6 Relevant company codes are set to Productive in the production environment.		
2.6.1 Transaction code OBR3 contains a list of company codes and whether they have been set to Productive. This information is also available in table T001 and can be viewed using transaction code SE16. Perform a review of this list. In instances where company codes that have not been set to Productive, the reasons should be investigated with management.		
3. Application Operations (Computing Center Management System)		
3.1 The Computing Center Management System is configured appropriately.		
3.1.1 Determine via inquiry whether transaction RZ04 was used to set up operations modes, instances and timetables to ensure that the CCMS displays meaningful data.		
3.1.2 Determine how the organization is monitoring its SAP R/3 system. Understand the policies, procedures, standards, and guidance regarding the execution of SAPSTART and STOPSAP programs or their equivalent in the organization's environment. Check that only authorized personnel may execute these programs.		
3.1.3 Generate a list of users with the ability to access the Alert Monitor by performing online access authorization testing for these authorization objects S_RZL_ADM, activity values 01 (administrator) and 03 (display) and transaction code, value AL01 (if a 3.x system) or RZ20 (if a 4.x system).		

Basis Security Cycle Audit Program

Control Objective/Test	Documentation / Matters Arising	COBIT Reference
<p>S_TCODE authorization object]. Where available, setting this parameter to Y allows the authorization check for transaction code to be switched off.)</p> <ul style="list-style-type: none"> Auth/system_access_check_off (This parameter switches off the automatic authorization check for particular ABAP/4 language elements [file operations, CPIC calls and calls to kernel functions]. This parameter may be used to ensure downward compatibility of the R/3 kernel [value=0, check remains active].) Rdisp/gui_auto_logout (specifies after how many minutes of inactivity will the user be automatically logged out) <p>Confirm that the system profile parameter files and default.pfl are protected from unauthorized access. Confirm that there is a mechanism/process to ensure that the profiles are regularly checked to ensure that they have not been changed inappropriately. Obtain any related change documentation and ensure that:</p> <ul style="list-style-type: none"> The documentation is authorized. Related log entries reflect the expected changes. A current printout of the RSUSR006 report is obtained and reviewed for unusual items or trends. Determine whether management has a process for frequent monitoring of unsuccessful login attempts and/or locked users via a review of this report. If yes, obtain details on the following frequency of monitoring. <p>Review a reasonable sample of previously followed up reports and assess the appropriateness of the follow-up on unusual findings. Run report RSUSR200. Review and follow up on:</p> <ul style="list-style-type: none"> Users with original passwords. Users who have not logged in during the last 60 days Users who have not changed their passwords in the last 60 days (or any duration that is appropriate for the organization). <p>Obtain a sample of user master records in the production environment and work with the authorization security administrator and the job descriptions to assess segregation of duties (refer chapter 4 for more guidance) and the appropriateness of the access granted.</p>		<p>DS5 ME1</p> <p>DS5</p> <p>PO4 DS5</p>
<p>3.4 Critical and sensitive transaction codes are locked in production.</p>		

Basis Security Cycle Audit Program

Control Objective/Test	Documentation / Matters Arising	COBIT Reference
3.4.1 Execute report RSUSR002 with the transaction code SM01 to provide a list of all users who have access to lock or unlock transaction codes in the system. Review and confirm this list with management to ensure only authorized users have access.		
3.4.2 Entering transaction code SM01 will display a list of transaction codes with a check box beside them. A cross in the check box indicates that the transaction code has been locked. Sensitive transaction codes should be reviewed to ensure they have been locked from user access. Such transaction codes include but are not limited to: <ul style="list-style-type: none"> • SCC5 Client Delete • SCC0 Client Copy (may overwrite the production client) • SM49 Execute Logical Commands (may allow pass through to operating system) • SM69 Execute Logical Commands (may allow pass through to operating system). 		
3.5 Users are prevented from logging in with trivial or easily guessable passwords.		
3.5.1 Based on the review of the key security policies, determine whether there are any character combinations (apart from the SAP R/3 standards) that the policy has prohibited from use. If yes, obtain a printout of the contents of table USR40 and confirm that the list of “illegal” words is contained therein.		PO6 DS5
3.6 SAP Router is configured to act as a gateway to secure communications into and out of the SAP R/3 environment.		
<i>SAP Router</i>		
3.6.1 Discuss with the operating system administrators the procedures surrounding changes to SAP Router and the procedures surrounding restarting SAP Router when it goes down.		AI4 DS5 M1 M2
3.6.2 Obtain a list of individuals with view and/or change access to the SAP Router binary. Review the list with key management and assess the appropriateness of the segregation of duties.		
3.6.3 Request an extract of the SAP Router permissions table (for example, execute the UNIX command SAP router -L <path>) from the operating system administrator. Review the permissions table with the operating systems administrator. Compare with network diagram to assess the appropriateness of the IP addresses and with change control documentation to confirm that management has appropriately authorized changes.		
3.6.4 If logging is Active, ascertain the frequency with which the logs are reviewed and followed up.		
3.6.5 Obtain a reasonable sample of the logs and review them with the operating systems administrator.		

Basis Security Cycle Audit Program

Control Objective/Test	Documentation / Matters Arising	COBIT Reference
3.7 Remote access by software vendors is controlled adequately.		
3.7.1 Determine the organization's approach to SAP Online Support Services (OSS). Verify the extent of access permitted and processes used to request, approve, authenticate, grant, monitor and terminate OSS access. Check that changes are subject to normal testing and migration controls.		DS2 DS5
3.7.2 Obtain a list of OSS users on the production client, enter transaction code OSS1 using the client's administrator ID. Click on the SAPNET icon followed by the administration icon. Perform an authorization analysis by authorization object view. This will provide a list of all users assigned OSS by authorization object. In particular, the users who have been assigned to Administration Authorization and Open Service Connections should be reviewed for reasonableness with management.		
3.8 SAP R/3 Remote Function Call (RFC) and Common Programming Interface—Communications (CPI-C) are secured.		
3.8.1 Ascertain whether the login information (dialog and/or non-dialog users) is stored and reviewed. Obtain a representative sample and review to ensure that dialog users are appropriate (i.e., valid employees with authorization) and that nondialog user IDs are appropriate. To do this, execute transaction code SM59. This will display the table RFCDES, which controls the communication between systems. The table lists the RFC destinations, which will include all R/3 connections that are on the system. Expand each of the R/3 connections and double click on each connection to verify that no dialog user ID is listed with its password.		PO2 AI4 DS5 ME1 ME2
3.8.2 Determine whether these systems are protected with the appropriate network measures (e.g., SAP Router/firewall/routers).		
3.8.3 Assess the strength/adequacy (i.e., robustness) of password measures to authenticate RFC connections.		
3.8.4 Confirm with R/3 security authorization manager that authority checks are included in functional modules called via RFC.		
3.8.5 Via report RSUSR002, identify users who have access to t-code SM59. Assess whether this access is appropriate (work with User Access Management).		
3.8.6 If using release 4.0 or higher, ascertain whether SNC protection has been applied to RFC calls. If yes, cross-reference to SNC documentation and testing performed earlier.		

Basis Security Cycle Audit Program

Control Objective/Test	Documentation / Matters Arising	COBIT Reference
3.9 Technology infrastructure is configured to secure communications and operations in the SAP R/3 environment.		
<i>Firewall</i>		
3.9.1 Discuss with the firewall administrators the procedures surrounding changes to the firewall rules and recovery of firewalls in the event of an outage.		A14 DS5 ME1 ME2
3.9.2 Obtain a list of individuals with view and/or change access to the firewall rules. Review the list with key management and assess the appropriateness of the segregation of duties.		DS5
3.9.3 Review the permissions table with the firewall administrator. Compare with network diagram to assess the appropriateness of the IP addresses.		DS13
3.9.4 If logging is set to Logging Active, ascertain the frequency with which the logs are reviewed and followed up.		
3.9.5 Obtain a reasonable sample of the logs and review them with the firewalls administrator.		
<i>Secure Network Communications (SNC)</i>		
3.9.6 Identify the communication paths that have been protected by SNC/external security product.		A14 DS5 ME1 ME2
3.9.7 Assess whether the level of protection is appropriate for each of the various communication paths. Use the requirements set out in the information security policy and various risk assessments to assist in the assessment.		
3.9.8 Review the configuration for each path with the Network Security Administrator for appropriateness.		
<i>Secure Store and Forward (SSF) Mechanisms and Digital Signatures</i>		
3.9.9 Determine whether there are any regional laws or regulations with which the organization must comply that govern the use of digital signatures. If yes, confirm that the organization is in compliance.		ME3 DS5
3.9.10 Determine whether the organization uses an external product for SSF. If yes: <ul style="list-style-type: none"> • Ascertain whether the organization uses hardware- or software-based keys. • Describe the controls surrounding issuance and changing of the public and private keys. • Ascertain whether the organization uses self-signed certificates or CA-signed certificates. 		PO2 DS5 DS13
3.9.11 If using release 4.5 or higher, determine whether SAPSECULIB is used as the default SSF provider. If yes, determine whether the file SAPSECU.pse is protected from unauthorized access.		DS5
<i>Workstation Security</i>		

Basis Security Cycle Audit Program

Control Objective/Test	Documentation / Matters Arising	COBIT Reference
<p>3.9.12 Via inspection, ensure that staff utilize any of the available security measures surrounding workstations/PCs (for example, screensavers, power-on passwords, third party security products, physical controls). Consider specifically, whether:</p> <ul style="list-style-type: none"> • Users are able to bypass screen saver/power-on passwords. • Screen savers activate automatically or are (as a rule) activated by users when they leave their work areas. 		DS5
<p>3.9.13 Regarding virus protection, determine whether:</p> <ul style="list-style-type: none"> • Virus scanners are used on the network and/or workstations. • Virus signatures are kept up-to-date. • There is a procedure for disseminating virus education to users. 		DS5 DS13
<p>3.9.14 Assess adequacy of physical controls. Consider specifically:</p> <ul style="list-style-type: none"> • Are the workstations in secure/restricted areas? • How is the area secured (e.g., security cards, keys, combination locks)? • Do individuals circumvent these controls (i.e., piggyback at entrance, prop open the door)? 		DS12 DS5
<i>Operating System and Database Security</i>		
<p>3.9.15 Work with the systems and database administrator to confirm that the passwords on the standard operating system and database user IDs have been changed, appropriate security parameters have been set and that appropriate security procedures are in place and operating.</p>		DS5

Basis Security Cycle Audit Program

Control Objective/Test	Documentation / Matters Arising	COBIT Reference
4. Application Security (Profile Generator and Security Administration)		
4.1 Duties within the security administration environment are segregated adequately.		
<p>4.1.1 Determine whether the system administrator tasks are segregated into the following administrator functions by generating user lists for the following authorizations using report RSUSR002.</p> <ul style="list-style-type: none"> • For the Profile Generator: <ul style="list-style-type: none"> - Create and change Activity Groups: Used to define and update Activity Groups. Use authorization S_USER_AGR with authorization field values of 01 and 02. This should be tested in conjunction with transaction code PFCG. - Transport Activity Group: Used to transport or activate Activity Groups to/in production. Use authorization S_USER_AGR with authorization field values of 21. This should be tested in conjunction with transaction code PFCG. - Transfer profiles to user master records: Used to assign or transfer authorization profiles into the user master records for the relevant activity group users. Use authorization S_USER_AGR with authorization field values of 22. This should be tested in conjunction with transaction code PFCG. • For manual maintenance: <ul style="list-style-type: none"> - User master maintenance— Authorizations: Defines and updates authorization profiles and authorizations. This should be tested in conjunction with transaction code SU03. Recommended settings: <ul style="list-style-type: none"> - Authorization Object: S_USER_PRO with authorization field values: 01, 02, 03, 06, 08 - Authorization Object: S_USER_AUT with authorization field values: 01, 02, 03, 06, 08 - User master maintenance—Activation: Activates authorization profiles and authorizations but cannot create or change them. This should be tested in conjunction with transaction code SU02 Recommended settings: <ul style="list-style-type: none"> - Authorization Object: S_USER_PRO with authorization field values of 06, 07 - Authorization Object: S_USER_AUT with authorization field values of 06, 07 		

Basis Security Cycle Audit Program

Control Objective/Test	Documentation / Matters Arising	COBIT Reference
<ul style="list-style-type: none"> - User master maintenance—User Groups: Defines, creates and edits user master records, edits the list of profiles in a user master record and sets user parameters. This should be tested in conjunction with transaction code SU01. Recommended settings: <ul style="list-style-type: none"> - Authorization Object: S_USER_GRP with authorization field values of: 01, 02, 03, 06, 22 - Authorization Object: S_USER_PRO with authorization field values of: 22 <p>Only the superuser should have authorization field values of 05 to lock and unlock users (prevent or allow logons) and change passwords.</p> <p>Hardcopies of RSUSR100/101/102 reports should be assessed for evidence of review and action by management.</p>		
<p>4.1.2 Test user access to effect mass changes to User Master Records authorization objects S_USER_GRP and S_USER_PRO with authorization field values of 01, 02, 05 and 06 and transaction codes SU10 (Delete/add a profile for all users) and SU12 (Delete all users).</p>		
<p>4.2 Adequate security authorization documentation is maintained.</p>		
<p>4.2.1 Select a random sample of authorized change documentation that pertains to changes to User Master Records. Run report RSUSR100 and assess whether the changes made are as documented.</p>		<p>AI6 DS5 ME1</p>
<p>4.2.2. Select a random sample of authorized change documentation that pertains to changes to profiles. Run report RSUSR101 and assess whether the changes made are as documented.</p>		<p>AI6 DS5 ME1</p>
<p>4.2.3 Select a random sample of authorized change documentation that pertains to changes to authorizations. Run report RSUSR102 and assess whether the changes made are as documented.</p>		<p>AI6 DS5 ME1</p>
<p>4.3 The Super User SAP* is secured properly.</p>		
<p>4.3.1 To determine whether the SAP* user has been locked, execute transaction SA38 (Reporting) with report name RSUSR002 and press F8. Enter SAP* in the User field and press F8. Verify that the SAP* Group field says SUPER. Click on the Other View button twice. The User status field for SAP* should say Locked.</p>		<p>DS5</p>

Basis Security Cycle Audit Program

Control Objective/Test	Documentation / Matters Arising	COBIT Reference
4.3.2 For SAP*, run report RSUSR003 to confirm that: <ul style="list-style-type: none"> • The ID has been deactivated in all clients and a new super user created. • The password has been changed from the default (i.e., not trivial). 		
4.4 Default users are secured properly.		
4.4.1 To test whether the default password has been changed for DDIC, SAPCPIC and Earlywatch, execute the SAP R/3 report RSUSR003 and determine if the default passwords have been changed. To determine whether the SAPCPIC and Earlywatch users have been locked, execute transaction SA38 (Reporting) with report name RSUSR002 and press F8. Enter the user name in the User field and press F8. Verify that the Group field says SUPER. Click on the Other View button twice. The User status field for should say Locked.		DS5
4.5 Access to powerful profiles is restricted.		
4.5.1 Review users assigned the privileged profiles of SAP_ALL and SAP_NEW for appropriateness. Users who have been assigned these superuser profiles should be assigned to user group Super or equivalent, which should be maintained by a limited number of Basis personnel only. To perform this test, execute transaction SA38 and enter report name RSUSR002. In the part noted as Selection Criteria for User enter SAP_ALL into the Profile field. Click on the button to the right of the text box. Enter SAP_NEW in the first empty text box. Click on Copy. By executing this report, all users who have superuser functionality will be listed. Other powerful profiles that should be checked for user access include S_A.USER and S_A.ADMIN (used to administer user master record authorizations). Check the user list identified by this test to ascertain whether individuals who have access to the above-mentioned functionality require this access, based on their job responsibilities and established policies procedures, standards and guidance.		

Basis Security Cycle Audit Program

Control Objective/Test	Documentation / Matters Arising	COBIT Reference
4.6 The authorization group that contains powerful users is restricted.		
4.6.1 Identify the system administrators within the organization and determine to which user groups their user IDs belong. Using report RSUSR002, review the system for users with the authorization object S_USER_AGR (Profile Generator environment) with the activity values 01,02, 21 and 22 and transaction code PFCG or the authorization object S_USER_GRP (manual maintenance) with the activity values of 01, 02, 05 and 06 and the transaction code SU01. The authorization field user group in user master maintenance should be similar to one of the values identified above. This would usually be the group SUPER or ITO-SYSTEM.		
4.7 Changes to critical SAP R/3 tables are logged by the system and reviewed by management.		
4.7.1 Review security procedures created by management that identify what tables are being logged and how often these logs are reviewed by management. For changes to be logged, the system profile parameter rec/client needs to be activated. This can be checked by reviewing the report RSPARAM and ensuring the value for this parameter is set to either ALL or to the client numbers that shall have table logging enabled. Enter transaction code SE16 and enter table TPROT as the object name along with an X in the PROTFLAG field. This will identify tables that have their changes logged. Run report RSTBPROT (table log) or RSTBHIST (table change analysis), which lists all changes to tables that have log data changes activated in their technical settings for the period specified. Take a representative sample of changes to these tables and compare these to the original supporting information/documentation. Obtain explanations for any changes for which supporting information or documentation is not available.		DS5
4.8 Changes made to the data dictionary are authorized and reviewed regularly.		
4.8.1 Understand management's policies and procedures regarding the review of data dictionary reports. Assess the adequacy of such policies, procedures, standards, and guidance, taking into account the: <ul style="list-style-type: none"> • Frequency with which the review is performed • Level of detail in the reports • Other independent data to which management compares the reports • Likelihood that the person performing the review will be able to identify exception items and • Nature of exception items that they can be expected to identify 		DS5

Basis Security Cycle Audit Program

Control Objective/Test	Documentation / Matters Arising	COBIT Reference
4.9 Log and trace files are configured appropriately and secured.		
<p>4.9.1 For security audit log, using release 4.0 or higher:</p> <ul style="list-style-type: none"> • Confirm that the security audit log has been activated by running the report RSPARAM and confirming the following parameter values: <ul style="list-style-type: none"> - Rsau/enable (activates logging on application server; if value is "0", it is not active) - Rsau/local/file (specifies the location of the log; confirms that it is appropriately located) - Rsau/max_diskspace/local (specifies the maximum size of the log; confirm that the size is adequate for the organization) • Obtain a listing of events that are logged (can be done via SM20). Review for appropriateness and link to required logging that may be specified in the security policies and standards. • Determine frequency and thoroughness of review of the logs. If possible, obtain a representative sample of the logs and assess the adequacy of the follow-up process and review for unusual items. 		DS5 ME1
<p>4.9.2 Review the system log:</p> <ul style="list-style-type: none"> • Run the report RSPARAM and review the following parameter values to obtain the locations of the log files: <ul style="list-style-type: none"> - Rslg/local/file (specifies the location of the local log on the application server; default: /usr/sap/<SID>/D20/log/SLOG<SAP_instance_#>) - Rslg/collect_daemon/host (specifies the application server that maintains the central log; default: <hostname of main instance>) - Rslg/central/file (specifies the location of the active file for the central log on the application server; default: /usr/sap/<SID>/SYS/global/ SLOGJ) - Rslg/central/old_file (specifies the location of the old file for the central log on the application server; default: /usr/sap/<SID>/SYS/global/ SLOGJO) - Rslg/max_diskspace/local (specifies the maximum length of the local log; default: 0.5 MB) - Rslg/max_diskspace/central (specifies the maximum length of the central log; default: 2 MB) - Rstr/file (the absolute pathname of the trace file: the trace filename is TRACE<R/3 System Number>) • Obtain a listing of events that are logged (can be done via SM21). Review for appropriateness 		DS5 DS10 DS11 DS13 ME1

Basis Security Cycle Audit Program

Control Objective/Test	Documentation / Matters Arising	COBIT Reference
<p>(including the size of each local and central log file) and link to required logging, which may be specified in the security policies and standards.</p> <ul style="list-style-type: none">• Determine frequency and thoroughness of review of the logs. If possible, obtain a representative sample of the logs and assess the adequacy of the follow-up process and review for unusual items.• Work with the operating system administrator to determine who has permissions to these files. Ensure the access is appropriate.		

Revenue Business Cycle ICQ						
Control Objective/Question		Response			Comment	COBIT Reference
		Yes	No	N/A		
1. Master Data Maintenance						
1.1	Changes made to master data are valid, complete, accurate and timely.					
1.1.1	Does relevant management, other than the initiators, check online reports of master data additions and changes back to source documentation on a sample basis?					DS11
1.1.2	Is access to create and change master data restricted to authorized individuals?					DS5
1.1.3	Have configurable controls been designed into the process to maintain the integrity of master data?					DS9
1.2	Master data remain current and pertinent.					
1.2.1	Does management periodically review master data to check their currency and ongoing pertinence?					DS11
1.2.2	Have appropriate credit limits been loaded for customers?					DS2
2. Sales Order Processing						
2.1	Sales orders are processed with valid prices and terms, and processing is complete, accurate and timely.					
2.1.1	Is the ability to create, change or delete sales orders, contracts, and delivery schedules restricted to authorized personnel?					DS5 AI6
2.1.2	Has the ability to modify sales pricing information been restricted to authorized personnel (refer master data integrity 1.1.2)?					DS5
2.1.2	Has the system been configured to limit the overwrite of prices compared to the price master data (SAP allows for no changes or a certain tolerance level)?					
2.1.3	Has the system been configured such that a sales order is blocked for further processing when the customer either gets too low a price or the price the sales person gives is not satisfactory (refer master data integrity 1.1.3)?					DS9
2.1.4	Are any fax orders reconciled periodically between the system and fax printouts to reduce the risk of duplicate orders?					PO8
2.2	Orders are processed within approved customer credit limits.					
2.2.1	Has the SAP R/3 software been configured to disallow the processing of sales orders that exceed customer credit limits?					DS9
2.3	Order entry data are completely and accurately transferred to the shipping and invoicing activities.					
2.3.1	Are reports of open sales documents prepared and monitored to check for timely shipment?					ME1 DS11
3. Shipping, Invoicing, Returns and Adjustments						
3.1	Controls are in place to prevent duplicate shipments or delay in the shipping of goods to customers.					
3.1.1	Does the SAP R/3 software match goods shipped to open line items on an open sales order and close each line item as the goods are shipped, thereby preventing further shipments for those line items?					DS6
	Are available shipping reports used to assist in controlling the shipping process?					PO11
3.2	Invoices are generated using authorized terms and prices and are calculated and recorded accurately.					

Revenue Business Cycle ICQ						
Control Objective/Question		Response			Comment	COBIT Reference
		Yes	No	N/A		
3.2.1	Does the SAP R/3 software automatically calculate invoice amounts and post invoices based on configuration data?					AI5
3.3	All goods shipped are invoiced in a timely manner.					
3.3.1	Are reports of goods shipped but not invoiced and un-invoiced debit and credit note requests prepared and investigated promptly?					DS5
3.3.2	Is the ability to create, change or delete picking slips, delivery notes and goods issues restricted to authorized personnel?					AI7
3.3.3	Are reports of invoices issued but not posted in FI prepared and investigated promptly?					AI7
3.4	Credit notes and adjustments to accounts receivable are accurately calculated and recorded.					
3.4.1	Is the ability to create, change or delete sales order return and credit requests and subsequent credit note transactions restricted to authorized personnel?					DS5
3.5	Credit notes for all goods returned and adjustments to accounts receivable are issued in accordance with organization policy and in a timely manner.					
3.5.1	Are sales order returns and credit request transactions matched to invoices?					
3.5.2	Have processing controls including a billing block or a delivery block been configured to block credit memos, or free of charge subsequent delivery documents that do not comply with the organization's policy on credits or returns?					AI2 DS9
4.	Collecting and Processing Cash Receipts					
4.1	Cash receipts are entered accurately, completely and in a timely manner.					
4.1.1	Are bank statements reconciled to the general ledger regularly?					
4.1.2	Has the system been configured to not allow processing of cash receipts outside of approved bank accounts?					DS9
4.1.3	Are customer open items and accounts receivable aging reports prepared and analyzed regularly?					AI4
4.2	Cash receipts are valid and are not duplicated.					
4.2.1	Are receipts allocated to a customer's account supported by a remittance advice that cross-references to an invoice number?					PO4
4.2.1	IS any unallocated cash or amounts received that are not cross-referenced to an invoice number immediately followed-up with the customer?					DS11
4.3	Cash discounts are calculated and recorded accurately.					
4.3.1	Have tolerance levels for allowable cash discounts and cash payment differences in the SAP R/3 system been defined such that amounts in excess of such levels cannot be entered into the SAP R/3 system?					PO9 PO8
4.4	Timely collection of cash receipts is monitored.					
4.4.1	As for 4.1.3, are customer open items and accounts receivable aging reports prepared and analyzed regularly?					PO4 AI4

Expenditure Business Cycle ICQ						
Control Objective/Question		Response			Comment	COBIT Reference
		Yes	No	N/A		
1. Master Data Maintenance						
1.1	Changes made to master data are valid, complete, accurate and timely.					
1.1.1	Does relevant management, other than the initiators, check online reports of master data additions and changes back to source documentation on a sample basis?					PO4 DS11
1.1.2	Is access to create and change master data restricted to authorized individuals?					DS5
1.1.2	Are user accounts validated against HR lists and access in alignment with role requirements?					
1.1.2	Are user accounts reviewed by management in line with organization policy?					
1.1.3	Have configurable controls been designed into the process to maintain the integrity of master data?					DS9
1.1.4	Is a naming convention used for vendor names (e.g., as per letterhead) to minimize the risk of establishing duplicated vendor master records?					DS2
1.2	Inventory master data remain current and pertinent.					
1.2.1	Does management periodically review master data to check their currency and ongoing pertinence?					DS11
2. Purchasing						
2.1	Purchase order entry and changes are valid, complete, accurate and timely.					
2.1.1	Is the ability to create, change, or cancel purchase requisitions, purchase orders and outline agreements (standing purchase orders) restricted to authorized personnel?					DS5 AI6
2.1.2	Does the SAP R/3 source list functionality only allow specified materials to be purchased from vendors included in the source list for the specified material?					DS2
2.1.3	Is the SAP R/3 release strategy used to authorize purchase orders, outline agreements (standing purchase orders), and unusual purchases (for example, capital outlays)?					AI6
2.2	Goods are only received for valid purchase orders and goods receipts are recorded completely, accurately and in a timely manner.					
2.2.1	When goods received are matched to open purchase orders, are receipts with no purchase order or that exceed the purchase order quantity by more than an established amount investigated?					DS6
2.2.1	Does management review exception reports of goods not received on time for recorded purchases?					DS5
2.2.2	Is the ability to input, change, or cancel goods received transactions restricted to authorized inbound logistics/raw materials personnel?					DS5
2.3	Defective goods are returned to suppliers in a timely manner.					

Expenditure Business Cycle ICQ						
Control Objective/Question		Response			Comment	COBIT Reference
		Yes	No	N/A		
2.3.1	Are rejected raw materials adequately segregated from other raw materials in a quality assurance bonding area and are they regularly monitored (assigned a movement type of 122) to ensure timely return to suppliers?					PO4
3.	Invoice Processing					
3.1	Amounts posted to accounts payable represent goods or services received.					
3.1.1	Is the ability to input, change, cancel or release vendor invoices for payment restricted to authorized personnel?					DS5
3.1.1	Is the ability to input vendor invoices that do not have a purchase order and/or goods receipt as support further restricted to authorized personnel?					DS5
3.2	Accounts payable amounts are calculated completely and accurately and recorded in a timely manner.					
3.2.1	Is the SAP R/3 software configured to perform a three-way match?					DS9
3.2.2	Is the SAP R/3 software configured with quantity and price tolerance limits?					DS9
3.2.3	Is the GR/IR account regularly reconciled?					DS11
3.2.4	Are reports of outstanding purchase orders regularly reviewed?					DS11
3.2.5	Does the SAP R/3 software restrict the ability to modify the exchange rate table to authorized personnel?					DS5
3.2.5	Does management approve values in the centrally maintained exchange rate table?					PO6
3.2.5	Does the SAP R/3 software automatically calculate foreign currency translation, based on values in the centrally maintained exchange rate table?					DS11
3.3	Credit notes and other adjustments are calculated completely and accurately and recorded in a timely manner.					
3.3.1	Is the ability to input, change, cancel or release credit notes restricted to authorized personnel?					DS5
4.	Processing Disbursements					
4.1	Disbursements made only for goods and services received are calculated, recorded and distributed to the appropriate suppliers accurately and in a timely manner.					
4.1.1	Does management approve the SAP R/3 payment run parameter specification?					PO6
4.1.2	Does the SAP R/3 software restrict to authorized personnel the ability to release invoices that have been blocked for payment, either for an individual invoice or for a specified vendor?					DS5

Inventory Business Cycle ICQ						
Control Objective/Question		Response			Comment	COBIT Reference
		Yes	No	N/A		
1. Master Data Maintenance						
1.1	Changes made to master data are valid, complete, accurate and timely.					
1.1.1	Does relevant management, other than the initiators, check online reports (using transaction code MM04) of master data additions and changes back to source documentation on a sample basis?					DS11
1.1.1	Do persons, independent of day-to-day custody or recording of inventory, count physical inventory on a continuous inventory basis?					ME2
1.1.1	Are monthly stock takes performed?					DS13
1.1.1	Where inventory adjustment forms are used, are they sequentially pre-numbered and is the sequence of such forms accounted for?					DS13
1.1.2	Have the creation and maintenance of master data been assigned and restricted to a dedicated area within the organization that understands how they may affect organizational processes and the importance of timely changes?					DS11
1.1.3	Have configurable controls been designed into the process to maintain the integrity of master data?					DS9
1.2	Inventory master data remain current and pertinent.					
1.2.1	Does management periodically review master data to check their currency and ongoing pertinence?					DS11
1.3	Settings or changes to the bill of materials or process order settlement rules are valid, complete, accurate and timely.					
1.3.1	Is the ability to create, change or delete the bill of materials restricted to authorized personnel?					AI6 DS5
1.3.2	Does relevant management, other than the initiators, check online reports of bill of materials or settlement rule additions and changes back to source documentation on a sample basis?					PO4
2.	Raw Materials Management					
2.1	Inventory is saleable, useable and adequately safeguarded.					
2.1.1	Are raw material requirements planned based on forecast orders and production plans and does the system functionality monitor and maintain inventory levels in accordance with organization policies?					DS1 DS3
2.1.1	Is the saleability of finished goods and usability of raw materials (including shelf life dates) assessed regularly during continuous inventory counts and are any goods or raw materials scrapped appropriately approved?					DS3
2.1.1	Does the quality department test a sample of raw materials and are rejected raw materials adequately segregated from other raw materials into a separate quality assurance bonding area and regularly monitored by the quality department personnel to ensure timely return to suppliers?					DS6

Inventory Business Cycle ICQ						
Control Objective/Question		Response			Comment	COBIT Reference
		Yes	No	N/A		
2.1.1	Does management review reports of slow-turnover inventory to ensure that it is still saleable or useable?					DS11
2.1.1	Do goods inwards/outwards personnel monitor all incoming and outgoing vehicles and ensure all goods leaving the premises are accompanied by duly completed documentation (e.g., Inter-company stock transfer order, delivery docket or goods returned note)?					DS3
2.1.1	Are goods delivered only to designated, physically secure loading bays within the warehouses and are they accepted only by authorized inbound logistic/raw materials personnel?					DS12 DS3
2.1.1	Is inventory stored in properly secured (gates locked at night and premises alarmed) environmentally conditioned warehouse locations where access is restricted to authorized personnel?					DS12
2.2	Raw materials are received and accepted only with valid purchase orders, and are recorded accurately and in a timely manner.					
2.2.1	Are goods received matched online with purchase order details and/or invoices?					DS13
2.2.1	Are long outstanding goods receipt notes, purchase orders, and/or invoices investigated timely and accrued as appropriate?					ME2
2.2.1	Are documents cancelled once matched or on payment of the invoice to prevent reuse?					PO8
2.2.1	Does management review exception reports of goods not received on time for recorded purchases?					ME1
2.2.2	When goods received are matched to open purchase orders, are receipts with no purchase order, or that exceed the purchase order quantity by more than an established amount, investigated?					PO8
2.2.3	Is the ability to input, change or cancel goods received transactions restricted to authorized inbound logistics/raw materials personnel?					DS5
2.2.4	Do persons independent of day-to-day custody or recording of inventory count physical inventory on a continuous-inventory basis?					PO4
2.2.4	Are inventory counts reconciled to inventory records and inventory records reconciled to the general ledger?					PO8
2.3	Defective raw materials are returned to suppliers in a timely manner.					
2.3.1	Are rejected raw materials adequately segregated from other raw materials in a quality assurance bonding area and are they regularly monitored (assigned a movement type of 122) to ensure timely return to suppliers?					PO4 M2

Inventory Business Cycle ICQ						
Control Objective/Question		Response			Comment	COBIT Reference
		Yes	No	N/A		
2.3.1	Are defective raw materials received from suppliers logged and recorded in the quality management system and is the log monitored to ensure that the defective goods are returned promptly and that credit is received in a timely manner?					DS2
3. Producing and Costing Inventory						
3.1	Transfers of materials to/from production, production costs and defective products/scrap are valid, recorded accurately, completely and in the appropriate period.					
3.1.1	Are inventories received, including transfers, counted and compared to the pick list (that is used to record movements of inventory in the financial records), by personnel in the area assuming responsibility for the inventory (e.g., production, goods storage), and are they recorded in the appropriate period?					DS13
3.1.1	Does management reconcile the goods-in-transit accounts regularly and do these accounts net off against other plants' outgoing goods-in-transit accounts?					PO8 DS3
3.1.1	Is an appropriate costing method used for raw materials at purchase order price and is the raw materials costing rolled into finished goods on a monthly basis?					DS13
3.1.1	Does the quality department, based on their knowledge of day-to-day activities, review records of scrapped and reworked items and check whether such items have been correctly identified and properly recorded in the appropriate accounting period?					DS3
3.1.1	Is the ability to create or change bills of material restricted to authorized personnel?					DS5 AI6
3.1.1	Is access to the material transfers and adjustments transactions appropriately restricted to authorized personnel?					DS5 AI6
3.1.1	Is the ability to create or change work centers restricted to authorized personnel?					DS5 AI6
3.1.2	Is the ability to create or change bills of material restricted to authorized personnel?					DS5 AI6
3.1.3	Is access to the material transfers and adjustments transactions appropriately restricted to authorized personnel?					DS5 AI6
3.1.4	Is the ability to create or change work centers restricted to authorized personnel?					DS5 AI6
4. Handling and Shipping Finished Goods						
4.1	Finished goods received from production are recorded completely and accurately in the appropriate period.					
4.1.1	Do persons independent of day-to-day custody or recording of inventory count physical inventory on a "Continuous Inventory" basis (refer 1.1.1)?					PO4
4.1.2	Is the changing of the settlement rules restricted to authorized users (refer 1.3.1)?					
4.2	Goods returned by customers are accepted in accordance with the organization's policies.					

Inventory Business Cycle ICQ						
Control Objective/Question		Response			Comment	COBIT Reference
		Yes	No	N/A		
4.2.1	Are quality-control inspections performed for finished goods returned by customers and/or received from production to assess whether such goods should be returned to inventory, reworked or scrapped?					M1 PO11
4.2.1	Does the QA team inspect the goods before a credit note can be issued?					
4.3	Shipments are recorded accurately, timely and in the appropriate period.					
4.3.1	Is access restricted to transferring stock between plants or executing the Post Goods Issue that creates the intercompany stock transfer advice and/or generates an electronic (EDI) or manual invoice?					DS12
4.3.1	Do outbound logistics/finished goods personnel monitor all incoming and outgoing vehicles and ensure all goods leaving the premises are accompanied by duly completed documentation (e.g., delivery docket or goods returned note)?					ME1
4.3.1	Before goods are shipped, are the details of the approved order compared to actual goods prepared for shipment by an individual independent of the order picking process?					PO4
4.3.2	Are the SAP R/3 reports (delivery due list and owed-to-customer report) of open sales documents prepared and monitored to ensure timely shipment?					DS11
4.3.2	Does the SAP R/3 account assignment configuration ensure that amounts for shipped goods are posted to the appropriate cost-of-goods-sold account?					

Basis Security ICQ						
Questions		Response			Comments	COBIT References
		YES	NO	N/A		
SAP R/3 Control Environment						
A	Establish control over information and information systems.					
A1	Has senior management established policies and standards governing the information systems of the entity?					PO6
A2	Has senior management assigned responsibilities for information, its processing, and its use?					PO2
A3	Is user management responsible for providing information that supports the entity's objectives and policies?					PO4
A4	Is user management responsible for the completeness, accuracy, authorization, security and timeliness of information?					PO8 DS11
A5	Is information systems management responsible for providing the information systems capabilities necessary for achievement of the defined information systems objectives and policies of the entity?					PO3 DS1 DS3
A6	Does senior management approve plans for development and acquisition of information systems?					PO5
A7	Does senior management monitor the extent to which development/configuration, operation, and control of information systems complies with established policies and plans?					ME1
A8	Are there outstanding audit findings from previous years?					ME1 ME2
B	Ensure that the information systems selected (whether new implementation or upgrade) meet the needs of the entity.					
B1	Are there procedures to ensure that decisions to develop or acquire information systems are made in accordance with the objectives and policies of the entity?					PO5 AI1
B2	Are there procedures to determine costs, savings and benefits before a decision is made to develop or acquire an information system?					AI1
B3	Are there procedures to ensure that the information system being developed or acquired meets user requirements?					AI1
B4	Are there procedures to ensure that information systems, programs, and configuration changes are adequately tested prior to implementation?					AI2 AI3
C	Ensure that the acquisition and configuration of information systems (whether new implementation or upgrade) are carried out in an efficient and effective manner.					
C1	Are standards established and enforced to ensure the efficiency and effectiveness of the systems acquisition and configuration process?					PO10 AI1 AI2
C2	Are there procedures to ensure that all systems are acquired and configured in accordance with the established standards?					AI2

Basis Security ICQ						
Questions		Response			Comments	COBIT References
		YES	NO	N/A		
C3	Is an approved acquisition plan (project plan) used to measure progress?					PO10
C4	Do all personnel involved in system acquisition and configuration activities receive adequate training and supervision?					PO7
D	Ensure the efficient and effective implementation or upgrade of information systems.					
D1	Has responsibility been assigned for implementation/configuration/upgrade of information systems?					PO4
D2	Are there procedures to ensure the efficiency and effectiveness of the implementation/configuration/upgrade of information systems?					AI4
D3	Are there procedures to ensure that information systems are implemented/configured/upgraded in accordance with the established standards?					AI3
D4	Is an approved implementation plan used to measure progress?					PO10
D5	Is effective control maintained over the conversion of information and the initial operation of the information system?					AI7
D6	Does user management participate in the conversion of data from the existing system to the new system?					AI7
D7	Is final approval obtained from user management prior to going live with a new information/upgraded system?					AI7
E	Ensure the efficient and effective maintenance of information systems.					
E1	Are there procedures to document and schedule all planned changes to information systems (including key ABAP programs)?					AI6
E2	Are there procedures to ensure that only authorized changes are initiated?					AI6
E3	Are there procedures to ensure that only authorized, tested and documented changes to information systems are accepted into the production client?					AI7 AI6
E4	Are there procedures to report planned information systems changes to information systems management and to the users affected?					AI6 DS8
E5	Are there procedures to allow for and control emergency changes?					AI6
E6	Are controls in place to prevent unauthorized changes to information systems (including key ABAP programs)?					AI6 DS5
F	Ensure that present and future requirements of users of information systems processing can be met.					
F1	Are there written agreements between users and information systems processing, defining the nature and level of services to be provided?					DS1
F2	Is there appropriate management reporting within information systems processing?					DS4 ME1

Basis Security ICQ						
Questions		Response			Comments	COBIT References
		YES	NO	N/A		
F3	Does information systems processing management keep senior and user management informed about technical developments that could support the achievement of the objectives and policies of the entity?					DS3 DS4
F4	Are there procedures/capacity planning activities to examine the adequacy of information processing resources to meet entity objectives in the future?					DS3
F5	Are there periodic planning activities to examine the adequacy of the volume of skilled staff (i.e., operating system, hardware, network, R/3) to support the systems now and in the future?					PO7
F6	Are there procedures for the approval, monitoring and control of the acquisition and upgrade of hardware and systems software?					AI3 DS3
F7	Is there a process for monitoring the volume of named and concurrent SAP R/3 users to ensure that the license agreement is not being violated?					ME3 DS3
F8	If the R/3 implementation is not at the most current version, is there a planned upgrade approach?					PO3 AI3 DS3
G	Ensure the efficient and effective use of resources within information systems processing.					
G1	Are budgets for information systems processing activities prepared on a regular basis?					PO5
G2	Are standards established and enforced to ensure efficient and effective use of information systems processing?					PO6
G3	Is there an incident management process that ensures that information-processing problems are detected and corrected on a timely basis?					DS5 DS10
G4	Are users of information systems processing facilities accountable for the resources used by them?					DS6
H	Ensure that there is an appropriate segregation of incompatible functions within the entity.					
H1	Does the organization structure established by senior management provide for an appropriate segregation of incompatible functions?					PO4
I	Ensure that all access to information and information systems is authorized.					
I1	Are there procedures to ensure that information and information systems are accessed in accordance with established policies and procedures?					DS5
J	Ensure that information systems processing is protected physically from unauthorized access and from accidental or deliberate loss or damage.					
J1	Are the database, application and presentation servers located in a physically separate and protected environment (i.e., a data center)?					DS12
J2	Are there procedures to ensure that environmental conditions (such as temperature and humidity) for hardware facilities are adequately controlled?					DS12
K	Ensure that information processing can be recovered and resumed after operations have been interrupted.					

Basis Security ICQ						
Questions		Response			Comments	COBIT References
		YES	NO	N/A		
K1	Are there procedures to allow information processing to resume operations in the event of an interruption?					DS4
K2	Are emergency, backup, and recovery plans documented and tested on a regular basis to ensure that they remain current and operational?					DS4
K3	Do personnel receive adequate training and supervision in emergency backup and recovery procedures?					DS4 DS7
L	Ensure that critical user activities can be maintained and recovered following interruption.					
L1	Are there backup and recovery plans to allow users of information systems to resume operations in the event of an interruption?					DS4
L2	Are all information and resources required by users to resume processing backed up regularly?					DS4 DS11
L3	Do user personnel receive adequate training and supervision in the conduct of the recovery procedures?					DS4 DS7
L4	Are application controls designed with regard to any weaknesses in segregation, security, development and processing controls that may affect the information system?					DS4 DS5
L5	Are there procedures to ensure that output is reviewed by users/management for completeness, accuracy and consistency?					DS4 ME1
L6	Is there some method of ensuring that control procedures relating to completeness, accuracy and authorization are ensured?					DS4 ME2
L7	Are there established policies and procedures for record retention?					DS4 PO6
1.	Application Installation (Implementation Guide and Organizational Model)					
1.1	Configuration changes are made in the development environment and transported to production.					
1.1.1	Has access to the Implementation Guide (IMG) in production been restricted?					DS5
1.1.2	Have the production client settings been flagged to not allow changes to programs and configuration?					DS9
1.2	The Organizational Model has been configured correctly to meet the needs of the organization.					
1.2.1	Was the Organizational Model well thought-out and agreed upon early in the implementation and did the relevant organization groups assist with key design decisions?					PO4
1.2.2	Has access to the organization configuration functionality been restricted?					DS5
1.3	Changes to critical number ranges are controlled.					
1.3.1	Has the SAP R/3 software security been appropriately configured to restrict the ability to change critical number ranges (i.e., company codes, chart of accounts and accounting period data)?					DS5
	Has the production environment been set to non-modifiable?					AI6
1.4	Access to system and customizing tables is restricted narrowly.					

Basis Security ICQ						
Questions		Response			Comments	COBIT References
		YES	NO	N/A		
1.4.1	Have all of the customized SAP R/3 tables been assigned to the appropriate authorization group?					DS5 PO4
1.4.2	Has the ability to modify critical tables been appropriately restricted in the production system?					DS5 AI6
2.	Application Development (ABAP/4 Workbench and Transport System)					
2.1	Application modifications are planned, tested and implemented in a phased manner.					
2.1.1	Are appropriate change controls procedures followed for all transports?					AI6
2.1.1	Has the production system change option been set to No Changes Allowed?					AI6
2.1.1	Has the ability to create versus release change requests been segregated?					PO4
2.2	Customized ABAP/4 programs are secured appropriately.					
2.2.1	Have customized ABAP/4 programs been assigned to authorization groups?					PO4 DS5
2.2.2	Has an authority-check statement been included within customized ABAP/4 programs so that the user's authority to access objects is checked at run time?					AI6
2.3	The creation or modification of programs is performed in the development system and migrated through the test system to production.					
2.3.1	Has access to directly change production source code within the production environment been controlled very tightly?					AI6
2.4	Access for making changes to the dictionary is restricted to authorized individuals.					
2.4.1	Has the ability to make changes to the SAP R/3 data dictionary been restricted and access privileges appropriately assigned based on job responsibilities?					PO4
2.5	Access to modify and develop queries is restricted.					
2.5.1	Have authorization groups for creating and running the ABAP/4 Queries been appropriately established in the SAP R/3 software in such a way that some end users can maintain and execute queries, while others can only execute existing queries?					PO4 DS5
2.6	Relevant company codes are set to Productive in the production environment.					
2.6.1	Have company codes that are working productively been set to Productive to reduce the risk that deletion programs may reset the company code data by mistake?					AI6 PO4
3.	Application Operations (Computing Center Management System)					
3.1	The Computing Center Management System is configured appropriately.					
3.1.1	Have operation modes, instances and the Computing Center Management System (CCMS) timetable been correctly defined, such that the CCMS display will be meaningful?					AI2
3.1.1	Is access to the system and start-up profiles tightly controlled?					AI6
3.1.1	Are change procedures followed strictly and changes to the profiles well documented?					AI6 DS11

Basis Security ICQ						
Questions		Response			Comments	COBIT References
		YES	NO	N/A		
3.1.1	Has access to the CCMS Alert Monitor been properly secured?					AI6 DS10
3.2	Batch processing operations are secured appropriately.					
3.2.1	Have batch input, batch administration and batch processing capabilities been restricted appropriately?					DS5 DS11
3.2.1	Have batch upload programs created to load initial master data and take on balances been deleted from the production environment following “go-live”?					AI7
3.3	Default system parameter settings have been reviewed and configured to suit the organization’s environment.					
3.3.1	During implementation, did the organization set the SAP R/3 system profile parameters to appropriate values?					AI4
3.4	Critical and sensitive transaction codes are locked in production.					
3.4.1	Have sensitive transaction codes been locked in the production environment and does the organization have procedures for locking and unlocking these transaction codes?					DS5 DS11
3.5	Users are prevented from logging in with trivial or easily guessable passwords.					
3.5.1	Has management set up a list of “illegal” passwords that users are not allowed to use?					DS5 DS13
3.6	SAP Router is configured to act as a gateway to secure communications into and out of the SAP R/3 environment.					
3.6.1	Is the network protected by SAP Router and a firewall?					DS5
3.6.1	Are appropriate change management procedures for any modifications to the SAP Router permission table in place and operating?					AI6
3.6.1	Is the SAP Router log file used to monitor remote communications activity?					DS5
3.6.1	Are Secure Network Communications (SNC) and an external security product used to protect the communication between the components of the R/3 system?					
3.7	Remote access by software vendors is controlled adequately.					
3.7.1	Is SAP or the support provider’s access restricted to a test/development environment, ideally on a separate file server from the production environment, activated only on request, and all activity logged and reviewed by an individual with the ability to understand the actions that have been taken?					DS5 AI6
3.7.2	Are changes subject to normal testing and migration controls before being implemented on the production system?					AI6
3.8	SAP R/3 Remote Function Call (RFC) and Common Programming Interface—Communications (CPI-C) are secured.					
3.8.1	Have the SAP R/3 RFC and CPI-C communications been secured so that any user who makes use of a connection will be prompted to enter a user name and password?					DS5

Basis Security ICQ						
Questions		Response			Comments	COBIT References
		YES	NO	N/A		
3.9	Technology Infrastructure is configured to secure communications and operations in the SAP R/3 environment.					
3.9.1	Has technology infrastructure been configured to secure communications and operations in the SAP R/3 environment? Consider the following areas: <ul style="list-style-type: none"> • Firewall • Secure Network Communications (SNC) • Secure Store and Forward (SSF) Mechanisms and digital signatures • Workstation security • Operating system and database security 					DS5 PO2
4.	Application Security (Profile Generator and Security Administration)					
4.1	Duties within the security administration environment are segregated adequately.					
4.1.1	Has the organization allocated the security administration function among different individuals?					PO4
4.2	Adequate security authorization documentation is maintained.					
4.2.1	Was original documentation of the SAP R/3 authorizations and their use developed and signed off by management during the implementation and has it been maintained adequately?					DS4 AI7
4.3	The super user SAP* is properly secured.					
4.3.1	Has the SAP* been assigned to the security administrators authorization group to prevent inadvertent deletion, the password changed from the default, all profiles and authorizations deleted and the user locked?					DS5
4.3.2	Has the system parameter (login/no_automatic_user_sapstar) been set?					AI6
4.4	Default users are secured properly.					
4.4.1	Have the passwords for the default users DDIC, SAPCPIC and Earlywatch been changed from the default?					DS5
4.5	Access to powerful profiles is restricted.					
4.5.1	Has a new super user account with the SAP_ALL and SAP_NEW profiles been created with a confidential ID and secret password for emergency use and has access to powerful profiles been restricted appropriately?					DS5 AI1
4.6	The authorization group that contains powerful users is restricted.					
4.6.1	Has the authorization group that contains powerful users been restricted to the new super user and a backup?					DS5 AI3
4.7	Changes to critical SAP R/3 tables are logged by the system and reviewed by management.					
4.7.1	Are all changes to the critical SAP R/3 tables logged by the system and does the periodic review of these logs form part of the security procedures for the organization?					AI6 DS11
4.8	Changes made to the data dictionary are authorized and reviewed regularly.					

Basis Security ICQ

Questions		Response			Comments	COBIT References
		YES	NO	N/A		
4.8.1	Are details of modifications to the data dictionary maintained and change control procedures followed?					AI6 DS11
	Are the SAP R/3 Data Dictionary Information System reports (DD reports) regularly generated and reviewed by management?					ME1 DS11
4.9	Log and trace files are configured and secured appropriately.					
4.9.1	Is logging appropriately configured and are log and trace files secured at the operating system level at the location specified within the system profile?					DS9