

**ISACA®**

ISACA (isaca.org) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

**Disclaimer**

ISACA has designed and created *SAP ERP Inventory Business Cycle Audit/Assurance Program* (the ‘Work’) primarily as an educational resource for assurance professionals. ISACA 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, assurance professionals should apply their own professional judgement 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, 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/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 SE in Germany and in several other countries. The publisher gratefully acknowledges SAP’s kind permission to use these trademarks and reproduce selected diagrams and screen shots in this publication. SAP SE is not the publisher of this book and is not responsible for it under any aspect of press law.

**Reservation of Rights**

© 2015 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorization of ISACA. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and noncommercial use and for consulting/advisory engagements, and must include full attribution of the material’s source. No other right or permission is granted with respect to this work.

**ISACA**

3701 Algonquin Road, Suite 1010

Rolling Meadows, IL 60008 USA

Phone: +1.847.253.1545

Fax: +1.847.253.1443

Email: *info@isaca.org*

Web site: *www.isaca.org*

Provide feedback: [*http://www.isaca.org/*](http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Align-Plan-and-Organise.aspx)*sap-erp-4th-edition*

Participate in the ISACA Knowledge Center: [*www.isaca.org/knowledge-center*](http://www.isaca.org/knowledge-center)

Follow ISACA on Twitter: [*https://twitter.com/ISACANews*](https://twitter.com/ISACANews)

Join ISACA on LinkedIn: ISACA (Official), [*http://linkd.in/ISACAOfficial*](http://linkd.in/ISACAOfficial)

Like ISACA on Facebook: [*www.facebook.com/ISACAHQ*](http://www.facebook.com/ISACAHQ)

# Acknowledgements

## ISACA wishes to recognize

### Project Leaders

### Benjamin Fitts, CPA, Deloitte & Touche LLP, USA

### Jacob Gregg, CISA, CISSP, Deloitte & Touche LLP, USA

### Michael Juergens, CISA, CGEIT, CRISC, CGAP, CIA, CRMA, Deloitte & Touche LLP, USA

### Michael Kosonog, CISA, CISSP, CITP, CPS, Deloitte & Touche LLP, USA

### Nancy A. Cohen, CPA, CIPP/US, ISACA, USA

### Eva Sweet, CISA, CISM, ISACA, USA

**Researchers**

Syed Aamir Aarfi, Deloitte & Touche LLP, USA

Carlos Amaya, CISA, Deloitte & Touche LLP, USA

Dan Argynov, PMP, Deloitte & Touche LLP, USA

Soumya Bikash Sen, CCSK, CISSP, Deloitte & Touche LLP, USA

David Bogatyrev, CISSP, CPA, Deloitte & Touche LLP, USA

Ramamallikarjunarao Chintakunta, CISSP, PMP, Deloitte & Touche LLP, USA

Kranthi Kumar Mitra Gangavarapu, CISSP, Deloitte & Touche LLP, USA

Venkat Praveen Juntipally, SAP FI, Deloitte & Touche LLP, USA

Sagnik Mukherjee, Deloitte & Touche LLP, USA

Sudhakar Sathiyamurthy, CISA CGEIT, CIPP, ITIL, Deloitte & Touche LLP, USA

Sonik Shah, Deloitte & Touche LLP, USA

Dennis Siau, CISA, CIA, CISSP, CPA, Deloitte & Touche LLP, USA

Shweta Srivastava, Deloitte & Touche LLP, USA

Anurag Tewary, Deloitte & Touche LLP, USA

Percy Tsai, CPA, Deloitte & Touche LLP, USA

Ravi Maddela Veeriah, Deloitte & Touche LLP, USA

Sravan Vemana, Deloitte & Touche LLP, USA

Anukool Vyas, Deloitte & Touche LLP, USA

**Expert Reviewers**

Steve Biskie, CISA, CGMA, CITP, CPA, High Water Advisors, USA

Adrienne C. Chung, CISA, CISM, CRISC, CA, CPA, Chung Consulting & Advisory Ltd., Canada

Mayank Garg, CISA, NetApp, USA

Ricci Ieong, Ph.D, CISA, CCSK, CEH, CISSP, eWalker Consulting (HK) Ltd., Hong Kong

Guhapriya Iyer, CISA, ACA, Grad.CWA, Cerebrus Consulting, India

Babu Jayendran, CISA, FCA, Babu Jayendran Consulting, India

Francis Kaitano, CISA, CISM, CISSP, ITIL, MCSD, SCF, New Zealand

Kamal Khan, CISA, CISSP, CITP, Saudi Aramco, Saudi Arabia

Jim Koveos, CISA, MBA, AmerisourceBergen, USA

Rajni Lalsinghani, CISA, CISM, Department of Human Services, Australia

Samuel LIM S.C., CISA, Auditor General's Office, Singapore

Alfonso Luque Romero, CISA, CISM, Banco de la Republica, Colombia

Lu Miao Chang, CISA, FCA, MCSE, SAP T/C, Auditor General’s Office, Singapore

Stane Moskon, CISA, CISM, OSIR d.o.o., Slovenia

Moonga Mumba, CISA, BBA, MSc Computer Forensics, SAP Cert., Zambia Revenue Authority, Zambia

Paul O'Donnell, Ernst & Young, Canada

Fernando Ortiz Guerrero, LIA, Ernst & Young, Mexico

John Ott, CISA, CISSP, CFE, CPA, LPT, AmerisourceBergen, US

Maria del Pilar Pliego Bermudez, CISA, CGEIT, CRISC, CPA, Ernst & Young, Mexico

Naved Rehman, CISA, CRISC, MS-IS, SAPauditCoach, US

Andriy Rybalchenko, CISA, CISM, LLC EastOne, Ukraine

Lily Shue, CISA, CISM, CGEIT, CRISC, LMS Associates, LLC, US

Sergio Raul Solis Garza, CISA, CGEIT, CRISC, ISO 27001 LA, Mexico

Jovari St. Victor, CISA, CPA, Sunera, LLC, US

Surapong Surabotsopon, CISA, CISM, CGEIT, CLS, ITIL, MCSE, mySAP (FICO), PMP,

KasikornBank, PCL, Thailand

Blanca Eva Villarreal Munoz, PMP, Ernst & Young, Mexico

Chakri Wicharn, CISA, CISM, CGEIT, CSPM, ITIL, PMP, Fuji Xerox Co., Ltd., Thailand

David Yeung, CISA, CFE, CIA, Management Consultant, Singapore

### ISACA Board of Directors

Robert E Stroud, CGEIT, CRISC, CA, USA, International President

Steven A. Babb, CGEIT, CRISC, ITIL, Vodafone, UK, Vice President

Garry J. Barnes, CISA, CISM, CGEIT, CRISC, Vital Interacts, Australia, Vice President

Robert A. Clyde, CISM, Clyde Computing LLC, USA, Vice President

Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, Six Sigma Black Belt, Dell, Spain, Vice President

Theresa Grafenstine, CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA, US House of Representatives, USA, Vice President

Vittal R. Raj, CISA, CISM, CGEIT, CRISC, CFE, CIA, CISSP, FCA, Kumar & Raj, India, Vice President

Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Past International President

Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Past International President

Debbie A. Lew, CISA, CRISC, Ernst & Young LLP, USA, Director

Frank K.M. Yam, CISA, CIA, FHKCS, FHKIoD, Focus Strategic Group Inc., Hong Kong, Director

Alexander Zapata Lenis, CISA, CGEIT, CRISC, ITIL, PMP, Grupo Cynthus S.A. de C.V., Mexico, Director

### Knowledge Board

### Steven A. Babb, CGEIT, CRISC, ITIL, Vodafone, UK, Chairman

### Rosemary M. Amato, CISA, CMA, CPA, Deloitte Touche Tohmatsu Ltd., The Netherlands

### Neil Patrick Barlow, CISA, CISM, CRISC, CISSP, Capital One, UK

### Charlie Blanchard, CISA, CISM, CRISC, CIPP/US, CIPP/E, CISSP, FBCS, ACA, Amgen Inc., USA

### Sushil Chatterji, CGEIT, Edutech Enterprises, Singapore

### Phil J. Lageschulte, CGEIT, CPA, KPMG LLP, USA

### Anthony P. Noble, CISA, Viacom, USA

### Jamie Pasfield, CGEIT, ITIL V3, MSP, PRINCE2, Pfizer, UK

Ivan Sanchez Lopez, CISA, CISM, ISO 27001 LA, CISSP, DHL Global Forwarding & Freight, Germany

### Guidance and Practices Committee

Philip J. Lageschulte, CGEIT, CPA, KPMG LLP, USA, Chairman

John Jasinski, CISA, CGEIT, ISO20K, ITIL Expert, SSBB, ITSMBP, USA

Yves Marcel Le Roux, CISM, CISSP, CA Technologies, France

Aureo Monteiro Tavares Da Silva, CISM, CGEIT, Brazil

Jotham Nyamari, CISA, Deloitte, USA

James Seaman, CISM, CRISC, A.Inst.IISP, CCP, QSA, RandomStorm Ltd, UK

Gurvinder Singh, CISA, CISM, CRISC, Australia

Siang Jun Julia Yeo, CISA, CRISC, CPA (Australia), MasterCard Asia/Pacific Pte. Ltd., Singapore

Nikolaos Zacharopoulos, CISA, CISSP, MerckGroup, Germany

**SAP ERP Inventory Business Cycle Audit/Assurance Program**

## Introduction

This document contains an example audit/assurance program, **based** **on** the generic structure developed in section 2B of *COBIT 5 for Assurance*[[1]](#footnote-1).

The engagement approach is based on, but **differs slightly** from the generic approach described in *COBIT 5 for Assurance:*

* The engagement approach described in this audit/assurance program **is focused on a business process** consequentlyno group of COBIT 5 processes dominates as primary processes and the lower-level processes are widespread, for evaluation purposes, the high-level COBIT 5 processes will be used as references.
* The assurance steps in this audit/assurance program are specific to the subject matter under review; therefore most of the assurance steps associated with the COBIT 5 processes identified in step A-3.2 have been omitted.Audit/assurance programs for these processes can be found in the ISACA web site at http://www.isaca.org/Knowledge-Center/Research/Pages/Audit-Assurance-Programs.aspx and can be included in this audit/assurance program depending on the necessity to include them and on resources availableprocess audit/assurance program**.**

# Assurance Engagement: SAP ERP Inventory Business Cycle

## *Assurance Topic*

The topic covered by this assurance engagement is the SAP ERP Inventory Business Cycle.

## *Business Impact and Risk*

SAP is widely used in many enterprises. Improper configuration of SAP could result in an inability for the enterprise to execute its critical processes.

Risk resulting from ineffective or incorrect configurations or use of SAP could result in some of the following:

* Disclosure of privileged information
* Single points of failure
* Low data quality
* Loss of physical assets
* Loss of intellectual property
* Loss of competitive advantage
* Loss of customer confidence
* Violation of regulatory requirements

## *Goal of the Review*

The objective of the SAP ERP audit/assurance review is to provide management with an independent assessment relating to the effectiveness of configuration and security of the enterprise’s SAP ERP architecture.

## *Scoping*

The review will focus on configuration of the relevant SAP ERP components and modules within the enterprise. The selection of the specific components and modules will be based upon the risk introduced to the enterprise by these components and modules.

From a process reference model (PRM) perspective, the following domains and processes apply to this audit and assurance programme:

* BAI02 *Manage requirements definition*
* BAI03 *Manage solution identification and build*
* DSS01 Manage Operations
* DSS05 *Manage security services*
* DSS06 *Manage business process controls*

*Minimum Audit Skills*

This review is considered highly technical. The IS audit and assurance professional must have an understanding of SAP best practice processes and requirements and be highly conversant in SAP tools, exposures and functionality. It should not be assumed that an audit and assurance professional holding the CISA designation has the requisite skills to perform this review.

*Testing SAP Security*

To determine which users have access to the relevant authorizations used in this audit program, use one of the following methods:

1. Use transaction code SUIM ➞ Users ➞ Users by Complex Selection Criteria

2. Use transaction code S\_BCE\_68001417

3. Use transaction code SA38 and the program RSUSR002. This method allows the user to specify a transaction code, a “valid to” date for users, and up to three other authorization objects (which also may be the authorization object for transaction code S\_TCODE) with associated values (two values under an AND relationship and three values under an OR relationship).

This method is generally sufficient for testing logical access security in relation to SAP ERP application infrastructure areas, but it is less suitable when large numbers of authorizations must be reviewed, such as in segregation of duties analysis and in some of the more complex areas of business cycle controls.

4. Use transaction code SUIM ➞ Users ➞ Users with Critical Authorizations (also accessible with program RSUSR008\_009\_NEW, which replaces programs RSUSR008 and RSUSR009 and transaction codes SU98 and/or SU99, for SAP Web AS 6.20 and later). This method offers improvements such as allowing differentiation between SAP defaults for critical data for different business areas, extended combination options for critical authorization data, improved performance, display of user filters and more analysis options for users in the result list.

| **Audit/Assurance Program for SAP ERP Inventory Business Cycle** |
| --- |
| **Phase A—Determine Scope of the Assurance Initiative** |
| **Ref.** | **Assurance Step** | **Guidance** | **Issue****Cross-reference** | **Comment** |
| **A-1** | Determine the **stakeholders** of the assurance initiative and their **stakes.** |  |  |  |
| A-1.1 | Identify the intended user(s) of the assurance report and their stake in the assurance engagement. This is the assurance objective. | **Intended user(s) of the assurance report** | **Board/audit committee:** Needs assurance over the effectiveness and efficiency of SAP ERP processes within the enterprise.**Chief financial officer (CFO):** Needs assurance that internal controls for financial applications work as intended.**Risk managers:** Need assurance that controls intended to address previously identified risk are working as intended. The results from the audit should be used to update the risk registry as needed.**Security managers:** Need to identify gaps in the security plans for SAP applications.**Owners / shareholders:**  Part or all of the SAP ERP assurance report may be included in statutory reporting.**Regulators:** Part or all of SAP ERP reporting may need to be disclosed to respective authorities. |  |  |
| A-1.2 | Identify the interested parties, accountable and responsible for the subject matter over which assurance needs to be provided. | **Accountable and responsible parties for the subject matter** | **Business executives:**  The individuals responsible for identifying requirements, approving design and managing performance. These people are, together with IT management, responsible for managing the correct and controlled use of SAP ERP services—in line with good practices.**Business process owners:** Responsible for defining application and technical requirements. Responsible for data classification.**IT management:**  Responsible for managing the correct and controlled use of SAP ERP services—together with the business executives. |  |  |
| **A-2** | Determine the assurance **objectives** based on assessment of the internal and external environment/context and of the relevant **risk** and related **opportunities** (i.e., not achieving the enterprise goals).  | **Assurance objectives** are essentially a more detailed and tangible expression of those enterprise objectives relevant to the subject of the assurance engagement.**Enterprise objectives** can be formulated in terms of the generic enterprise goals (COBIT 5 framework) or they can be expressed more specifically.**Objectives of the assurance engagement** can be expressed using the COBIT 5 enterprise goals, the IT-related goals (which relate more to technology), information goals or any other set of specific goals.**Objectives of the assurance engagement** will consider all three value objective components, i.e., delivering benefits that support strategic objectives, optimizing the risk that strategic objectives are not achieved and optimizing resource levels required to achieve the strategic objectives. |  |  |
| A-2.1 | Understand the enterprise strategy and priorities.  | *Inquire with executive management or through available documentation (corporate strategy, annual report, etc.) about the enterprise strategy and priorities for the coming period, and document them.* |  |  |
| A-2.2 | Understand the internal context of the enterprise. | *Identify all internal environmental factors that could influence the performance and contents of the* ***SAP ERP Inventory Module****.** Review prior report, if one exists, verify completion of any agreed-on corrections, and note remaining deficiencies*.* **Determine whether:**
	+ Senior management has assigned responsibilities for information, its processing, and its use
	+ User management is responsible for providing information that supports the entity’s objectives and policies
	+ Information systems management is responsible for providing the capabilities necessary for the achievement of the defined information systems objectives and the policies of the entity
	+ Senior management approves plans for development and acquisition of information systems
	+ There are procedures to ensure that the information system being developed or acquired meets user requirements
	+ There are procedures to ensure that information systems, programs and configuration changes are tested adequately prior to implementation
	+ All personnel involved in the system acquisition and configuration activities receive adequate training and supervision
	+ There are procedures to ensure that information systems are implemented/configured/upgraded in accordance with the established standards
	+ User management participates in the conversion of data from the existing system to the new system
	+ Final approval is obtained from user management prior to going live with a new information/upgraded system
	+ There are procedures to document and schedule all changes to information systems (including key ABAP programs)
	+ There are procedures to ensure that only authorized changes are initiated
	+ There are procedures to ensure that only authorized, tested and documented changes to information systems are accepted into the production client
	+ There are procedures to allow for and control emergency changes
	+ There are procedures for the approval, monitoring and control of the acquisition and upgrade of hardware and systems software
	+ There is a process for monitoring the volume of named and concurrent SAP ERP users to ensure that the license agreement is not being violated
	+ The organizational structure, established by senior management, provides for an appropriate segregation of incompatible functions
	+ The database, application and presentation servers are located in a physically separate and protected environment (i.e., a data center)
	+ Emergency, backup and recovery plans are documented and tested on a regular basis to ensure that they remain current and operational
	+ Backup and recovery plans allow users of information systems to resume operations in the event of an interruption
	+ Application controls are designed with regard to any weaknesses in segregation, security, development and processing controls that may affect the information system
	+ Access to the Implementation Guide (IMG) during production has been restricted
	+ The production client settings have been flagged to not allow changes to programs and configuration
* Identify the significant risk and determine the key controls
	+ Develop a high-level process flow diagram and overall understanding of the Inventory Module, including the following subprocesses:
	1. Master data maintenance
	2. Raw materials management
	3. Producing and costing inventory
	4. Handling and shipping finished goods
	+ Assess the key risk, determine key controls or control weaknesses, and test controls (refer to the sample testing program below and chapter 4 for techniques for testing configurable controls and logical access security) regarding the following factors:
1. The controls culture of the organization (e.g., a just-enough-control philosophy).
2. The need to exercise judgment 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.)
* Gain an understanding of the SAP ERP environment (The same background information obtained for the SAP ERP Basis Security audit plan is required for and relevant to the business cycles)

**In particular, the following information is important:*** + Version and release of SAP ERP implemented
	+ Total number of named users (for comparison with logical access security testing results)
	+ Number of SAP instances and clients
	+ Accounting period, company codes and chart of accounts
	+ Identification of the components being used (Human Capital Management, Financials, Operations, Corporate Services)
	+ 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 risk
	+ Copies of the organization’s key security policies and standards

**Obtain details of the following:*** + Organizational Management Model as it relates to sales/revenue activity, i.e., sales organizational unit structure in SAP ERP and company sales organizational chart (required when evaluating the results of access security control testing)
	+ An interview of the systems implementation team, if possible, and process design documentation for sales and distribution
 |  |  |
| A-2.3 | Understand the external context of the enterprise. | *Identify all external environmental factors that could influence the* ***performance and contents of the SAP ERP Inventory Module****.* |  |  |
| A-2.4 | Given the overall assurance objective, translate the identified strategic priorities into concrete objectives for the assurance engagement. | The following goals are retained as key goals to be supported, in reflection of enterprise strategy and priorities:  |  |  |
| **Key goals** | Enterprise goals:* EG03 Managed business risk (safeguarding of assets)
* EG04 Compliance with externals laws and regulations
* EG07 Business service continuity and availability
* EG11 Optimisation of business process functionality
* EG15 Compliance with internal policies

IT-related goals:* ITG01 Alignment of IT and business strategy
* ITG02 IT compliance and support for business compliance with external laws and regulations
* ITG04 Managed IT-related business risk
* ITG07 Delivery of IT services in line with business requirements
* ITG08 Adequate use of applications, information and technology solutions
* ITG09 IT Agility
* ITG10 Security of information, processing infrastructure and applications
* ITG12 Enablement and support of business processes by integrating applications and technology into business processes
* ITG14 Availability of reliable and useful information for decision making
* ITG15 IT compliance with internal policies
* ITG16 Competent and motivated business and IT personnel
 |  |  |
| **Additional goals** |  |  |  |
| A-2.5 | Define the organizational boundaries of the assurance initiative. | *Describe the organizational boundaries of the assurance engagement, i.e., to which organizational entities the review is limited. All other aspects of scope limitation are identified during phase A-3.** The review must have a defined scope. The reviewer must understand the operating environment and prepare a proposed scope, subject to a later risk assessment.
* Obtain information and form an understanding of the business reasons underlying the audit.
* Identify the senior business resources responsible for the review.
* Identify the senior IT audit/assurance resource responsible for the review.
* Establish the process for suggesting and implementing changes to the audit/assurance program, and list the authorizations required.
* Identify any limitations and/or constraints affecting the audit of specific systems and subsystems.
* Identify and third party services, applications, platforms and infrastructure elements that may not be or only partially be accessible.
* Identify any legal, regulatory or contractual constraints on audit.
* Identify any industrial relations based or end user based audit constraints.
 |  |  |
| **A-3** | Determine the **enablers** in scope and the instance(s) of the enablers in scope. | COBIT 5 identifies seven enabler categories. In this section all seven are covered, and the assurance professional has the opportunity to select enablers from all categories to obtain the most comprehensive scope for the assurance engagement. |  |  |
| A-3.1 | Define the **Principles, Policies and Frameworks** in scope. | Guiding principles and policies include:* Policy for Master Data Maintenance
* ISMS policy
* Legal and regulatory compliance requirements
 |  |  |
| A-3.2 | Define which **Processes** are in scope of the review. Processes will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on:* Achievement of process goals
* Application of process good practices
* Existence and quality of work products (inputs and outputs) (insofar not covered by the information items assessments)
 | *COBIT 5: Enabling Processes* distinguishes a governance domain with a set of processes and a management domain, with four sets of processes. The processes in scope are identified using the goals cascade and subsequent customization. The resulting lists contain key processes and additional processes to be considered during this assurance engagement. Available resources will determine whether they can all be effectively assessed. |  |  |
| **Key processes** | * Master Data Maintenance
* Raw Materials Management
* Producing and Costing Inventory
* Handling and Shipping Finished Goods
 |  |  |
| **Additional processes** | * APO01 Mange the IT Management Framework
* APO06 Manage Budget and Cost
* APO07 Manage Human Resources
* APO11 Manage Quality
* APO12 Manage Risk
* APO13 Manage Security
* BAI02 Manage Requirements Definition
* BAI03 Manage Solution Identification and Build
* BAI04 Manage Availability and Capacity
* BAI06 Manage Changes
* DSS01 Manage Operations
* DSS05 Manage Security Services
* DSS06 Manage Business Process Controls
* MEA01 Monitor, Evaluate and Assess Performance and Conformance
 |  |  |
| A-3.3 | Define which **Organisational Structures** will be in scope. Organisational Structures will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on:* Achievement of Organisational Structure goals, i.e., decisions
* Application of Organisational Structures good practices
 | Based on the key processes identified in A-3.2, the following Organisational Structures and functions are considered to be in scope of this assurance engagement, and available resources will determine which ones will be reviewed in detail. |  |  |
| **Key Organisational Structures** | * Warehouse
* Quality
* Shipping
* Financial accounting
* Tax department
* General Accounting
* Treasury
 |  |  |
| **Additional Organisational Structures** | * IT Operations
* Master data maintenance group
* SAP ERP support and maintenance
* SAP training
* Tax department
* Change Management Office
 |  |  |
| A-3.4 | Define the **Culture, Ethics and Behaviour** aspects in scope. | In the context of this engagement, the following enterprisewide culture and behaviours are in scope:* Risk and compliance aware culture
* Enabling of continuous improvement
* Accountability
* Discipline to follow instructions
 |  |  |
| A-3.5 | Define the **Information items** in scope.Information items will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on:* Achievement of Information goals, i.e., quality criteria of the information items
* Application of Information good practices (Information attributes)
 | Based on the subject matter of this audit/assurance program, the following Information items have been identified as key items. |  |  |
| **Key Information Items** | * Data integrity procedures
* Data classification guidelines
* Data security and control guidelines
* Assigned responsibilities for resource management
* Access logs
* Allocated roles and responsibilities
* Allocated levels of authority
* Allocated access rights
* Evidence or error correction and remediation
* Error reports and root cause analysis
* Retention requirements
* Record of transactions
* Training manuals
* Job aids
 |  |  |
| **Additional Information Items** | * Organizational charts
 |  |  |
| A-3.6 | Define the **Services, Infrastructure and Applications** in scope. | In the context of this assignment, and taking into account the goals identified in A-2.4, the following services and related applications or infrastructure could be considered in scope of the review:* SAP ERP System
* Master data maintenance
* Change management
* SAP training
 |  |  |
| A-3.7 | Define the **People,** **Skills and Competencies** in scope.Skill sets and competencies will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on:* Achievement of skills set goals
* Application of skills set and competencies good practices
 | In the context of this engagement, taking into account key processes and key roles, the following skill sets are included in scope:* Proficiency using the SAP Materials Management Module
* Master data management skills
* Materials management skills and experience
* Proficiency running SAP reports
* Understanding of data classification policies
* Understanding of data integrity procedures
 |  |  |

| **Audit/Assurance Program for SAP ERP Inventory Business Cycle** |
| --- |
| **Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment** **Metrics** |
| **Ref.** | **Assurance Steps and Guidance** | **Issue****Cross-reference** | **Comment** |
| **B-1** | **Agree on metrics and criteria for enterprise goals and IT-related goals. Assess enterprise goals and IT-related goals.** |  |  |
| B-1.1 | Obtain (and agree on) metrics for enterprise goals and expected values of the metrics. Assess whether enterprise goals in scope are achieved.*Leverage the list of suggested metrics for the enterprise goals to define, discuss and agree on a set of relevant, customized metrics for the enterprise goals, taking care that the suggested metrics are driven by the performance of the topic of this assurance initiative.**Next, agree on the expected values for these metrics, i.e., the values against which the assessment will take place.* |  |  |
| The following metrics and expected values are agreed on for the key enterprise goals defined in step A-2.4. |  |  |
| **Enterprise Goal** | **Metric** | **Expected Outcome (Ex)** | **Assessment Step** |  |  |
| EG03 Managed business risk (safeguarding of assets)  | * Percent of critical business objectives and services covered by risk assessment
* Ratio of significant incidents that were not identified in risk assessments vs. total incidents
* Frequency of update of risk profile
 | *Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.* | *In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.* |  |  |
| EG04 Compliance with externals laws and regulations | * Cost of regulatory non-compliance, including settlements and fines
* Number of regulatory non-compliance issues causing public comment or negative publicity
* Number of regulatory non-compliance issues relating to contractual agreements with business partners
 | *Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.* | *In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.* |  |  |
| EG07 Business service continuity and availability | * Number of customer service interruptions causing significant incidents
* Business cost of incidents
* Number of business processing hours lost due to unplanned service interruptions
* Percent of complaints as a function of committed service availability targets
 | *Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.* | *In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.* |  |  |
| EG11 Optimisation of business process functionality | * Frequency of business process capability maturity assessments
* Trend of assessment results
* Satisfaction levels of board and executives with business process capabilities
 | *Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.* | *In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.* |  |  |
| EG15 Compliance with internal policies | * Number of incidents related to non-compliance to policy
* Percent of stakeholders who understand policies
* Percent of policies supported by effective standards and working practices
 | *Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.* | *In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.* |  |  |
| B-1.2 | Obtain (and agree on) metrics for IT-related goals and expected values of the metrics and assess whether IT-related goals in scope are achieved. |  |  |
| The following metrics and expected values are agreed for the key IT-related goals defined in step A-2.4. |  |  |
| **IT-related Goal** | **Metric** | **Expected Outcome (Ex)** | **Assessment Step** |  |  |
| ITG01 Alignment of IT and business strategy | * Percent of enterprise strategic goals and requirements supported by IT strategic goals
* Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services
* Percent of IT value drivers mapped to business value drivers
 | *Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.* | *In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.* |  |  |
| ITG02 IT compliance and support for business compliance with external laws and regulations | * Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss
* Number of IT-related non-compliance issues reported to the board or causing public comment or embarrassment
* Number of non-compliance issues relating to contractual agreements with IT service providers
* Coverage of compliance assessments
 | *Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.* | *In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.* |  |  |
| ITG04 Managed IT-related business risk | * Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment
* Number of significant IT-related incidents that were not identified in risk assessment
* Percent of enterprise risk assessments including IT-related risk
* Frequency of update of risk profile
 | *Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.* | *In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.* |  |  |
| ITG07 Delivery of IT services in line with business requirements | * Number of business disruptions due to IT service incidents
* Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels
* Percent of users satisfied with the quality of IT service delivery
 | *Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.* | *In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.* |  |  |
| ITG08 Adequate use of applications, information and technology solutions | * Percent of business process owners satisfied with supporting IT products and services
* Level of business user understanding of how technology solutions support their processes
* Satisfaction level of business users with training and user manuals
* Net present value (NPV) showing business satisfaction level of the quality and usefulness of the technology solutions
 | *Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.* | *In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.* |  |  |
| ITG09 IT Agility | * Level of satisfaction of business executives with IT’s responsiveness to new requirements
* Number of critical business processes supported by up-to-date infrastructure and applications
* Average time to turn strategic IT objectives into an agreed-on and approved initiative
 | *Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.* | *In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.* |  |  |
| ITG10 Security of information, processing infrastructure and applications | * Number of security incidents causing financial loss, business disruption or public embarrassment
* Number of IT services with outstanding security requirements
* Time to grant, change and remove access privileges, compared to agreed-on service levels
* Frequency of security assessment against latest standards and guidelines
 | *Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.* | *In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.* |  |  |
| ITG12 Enablement and support of business processes by integrating applications and technology into business processes | * Number of business processing incidents caused by technology integration errors
* Number of business process changes that need to be delayed or reworked because of technology integration issues
* Number of IT-enabled business programmes delayed or incurring additional cost due to technology integration issues
* Number of applications or critical infrastructures operating in silos and not integrated
 | *Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.* | *In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.* |  |  |
| ITG14 Availability of reliable and useful information for decision making | * Level of business user satisfaction with quality and timeliness (or availability) of management information
* Number of business process incidents caused by non-availability of information
* Ratio and extent of erroneous business decisions where erroneous or unavailable information was a key factor
 | *Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.* | *In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.* |  |  |
| ITG15 IT compliance with internal policies | * Number of incidents related to non-compliance to policy
* Percent of stakeholders who understand policies
* Percent of policies supported by effective standards and working practices
* Frequency of policies review and update
 | *Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.* | *In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.* |  |  |
| ITG16 Competent and motivated business and IT personnel | * Percent of staff whose IT-related skills are sufficient for the competency required for their role
* Percent of staff satisfied with their IT-related roles
* Number of learning/training hours per staff member
 | *Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.* | *In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.* |  |  |

| **Audit/Assurance Program for SAP ERP Inventory Business Cycle** |
| --- |
| **Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment** **Principles, Policies and Frameworks** |
| **Ref.** | **Assurance Steps and Guidance** | **Issue****Cross-reference** | **Comment** |
| **B-2** | Obtain an understanding of the **Principles, Policies and Frameworks** in scope and set suitable assessment criteria.Assess Principles, Policies and Frameworks**.** |  |  |
| **Principles, policies and frameworks: Policy for Master Data Maintenance** |
| B-2.1a | Understand the **Principles, Policies and Frameworks context**.*Obtain and understanding of the overall system of internal control and the associated Principles, Policies and Frameworks* |  |  |
| B-2.2a | Understand the stakeholders of the **Principles, Policies and Frameworks**. *Understand the stakeholders in the policies. The stakeholders for the policies include those setting the policies and those who need to be in compliance with the policies.* |  |  |
| B-2.3a | Understand the **goals** for the **Principles, Policies and Frameworks**, and the related **metrics** and agree on expected values.Assess whether the **Principles, Policies and Frameworks** goals (outcomes) are achieved, i.e., assess the effectiveness of the **Principles, Policies and Frameworks**. |  |  |
| Goal: The organization has defined, disseminated and deployed management policies supporting **SAP master data maintenance**. | Perform the assurance steps using the example criteria described below. |  |  |
| **Goal** | **Criteria** | **Assessment Step** |  |  |
| Comprehensiveness | The set of policies is comprehensive in its coverage. | Verify that the set of policies is comprehensive in its coverage. |  |  |
| Currency | The set of policies is up to date. This at least requires:* A regular validation of all policies whether they are still up to date
* An indication of the policies’ expiration date or date of last update
 | Verify that the set of policies is up to date. This at least requires:* A regular validation of all policies whether they are still up to date
* An indication of the policies’ expiration date or date of last update
 |  |  |
| Flexibility | The set of policies is flexible. It is structured in such a way that it is easy to add or update policies as circumstances require. | Verify the flexibility of the set of policies, i.e., that it is structured in such a way that it is easy to add or update policies as circumstances require. |  |  |
| Availability | * Policies are available to all stakeholders.
* Policies are easy to navigate and have a logical and hierarchical structure.
 | * Verify that policies are available to all stakeholders.
* Verify that policies are easy to navigate and have a logical and hierarchical structure.
 |  |  |
| B-2.4a | Understand the life cycle stages of the **Principles, Policies and Frameworks**, and agree on the relevant criteria.Assess to what extent the **Principles, Policies and Frameworks** life cycle is managed.*The life cycle of the IT-related policies is managed by the Process APO01. The review of this life cycle is therefore equivalent to a process review of process APO01* Manage the IT management framework*.* |  |  |
| B-2.5a | Understand good practices related to the **Principles, Policies and Frameworks** and expected values. Assess the Principles, Policies and Frameworks design, i.e., assess the extent to which expected good practices are applied.*The assurance professional will, by using appropriate auditing techniques assess the following aspects.* |  |  |
| **Good Practice** | **Criteria** | **Assessment Step** |  |  |
| Scope and validity | The scope is described and the validity date is indicated. | Verify that the scope of the framework is described and the validity date is indicated. |  |  |
| Exception and escalation | * The exception and escalation procedure is explained and commonly known.
* The exception and escalation procedure has not become the de facto standard procedure.
 | * Verify that the exception and escalation procedure is described, explained and commonly known.
* Through observation of a representative sample, verify that the exception and escalation procedure has not become *de facto* standard procedure.
 |  |  |
| Compliance | The compliance checking mechanism and non-compliance consequences are clearly described and enforced. | Verify that the compliance checking mechanism and non-compliance consequences are clearly described and enforced. |  |  |
| **B-2.1 to B-2.5** | Repeat steps B-2.1 through B-2.5 for all remaining **Principles, Policies and Frameworks** in scope. |  |  |
| Repeat the steps described above for the remaining Principles, Policies and Frameworks: * ISMS policy
* Legal and regulatory compliance requirements
 |  |  |

| **Audit/Assurance Program for SAP ERP Inventory Business Cycle** |
| --- |
| **Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment****Processes** |
| **Ref.** | **Assurance Steps and Guidance** | **Issue****Cross-reference** | **Comment** |
| **B-3** | Obtain understanding of the **Processes** in scope and set suitable assessment criteria: for each process in scope (as determined in step A-3.2), additional information is collected and assessment criteria are defined. Assess the Processes. |  |  |
| **SAP ERP Inventory process[[2]](#footnote-2): Master data maintenance** |
| B-3.1a | Understand the **Process context.** |  |  |
| B-3.2a | Understand the **Process purpose.** |  |  |
| B-3.3a | Understand all process **stakeholders** and their roles. This is equivalent to understanding the real RACI chart of the process.*Leverage the COBIT 5 RACI charts for the processes in scope to identify any additional stakeholders that will need to be involved in the assessment. In this assurance step, the translation is made between the theoretical RACI chart entry and the real enterprise.* |  |  |
| The stakeholders of the process are already defined in the RACI chart as a result of step A-3.3. In addition to those stakeholders, this process relies also on the following function(s), which therefore will need to be involved during the assurance engagement:**Master data maintenance** stakeholders:  |  |  |
| B-3.4a | Understand the **Process goals** and related **metrics[[3]](#footnote-3)** and define expected Process values (criteria), and assess whether the Process goals are achieved, i.e., assess the effectiveness of the process. |  |  |
| The Process **Master data maintenance** has three defined process goal. | The following activities can be performed to assess whether the goals are achieved. |  |  |
| **Process Goal** | **Related Metrics** | **Criteria/Expected Value** | **Assessment Step** | **Issue****Cross-reference** | **Comment** |
| Master data records are valid, complete, accurate and timely | *Determine the metrics that can be used to assess the achievement of the Process goals.* | *Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.* | *In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.* |  |  |
| Inventory master data remains current and pertinent | *Determine the metrics that can be used to assess the achievement of the Process goals.* | *Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.* | *In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.* |  |  |
| Settings or changes to the bill of materials or process order settlement rules are valid, complete, accurate and timely | *Determine the metrics that can be used to assess the achievement of the Process goals.* | *Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.* | *In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.* |  |  |
| B-3.5a | Agree on suitable criteria to evaluate all processes in scope of the assurance engagement: Define and agree on the reference process, i.e., determine which base practices a process should at least include. (This usually is just a confirmation of the COBIT 5 processes already identified, unless there is reason for using a different reference process.)Agree on the process practices that should be in place (process design).Assess the **process design**, i.e., assess to what extent: * Expected process practices are applied.
* Accountability and responsibility are assigned and assumed.

Evaluate **Master data maintenance** |  |  |
| **COBIT 5 Processes[[4]](#footnote-4)** are described in *COBIT 5: Enabling Processes*. Each Process requires a number of management practices to be implemented, as described in the process description in the same guide. These are: * A sound process design

The reference against which the process will be assessed in phase B with the criteria as mentioned, i.e., all management practices are expected to be fully implemented. |  |  |
| **Reference****Process** | Master data maintenance | Criteria: 1.1 Changes made to master data are valid, complete, accurate and timely.1.2 Inventory master data remains current and pertinent.1.3 Settings or changes to the bill of materials or process order settlement rules are valid, complete, accurate and timely. |  |  |
| **Reference****Process Practices[[5]](#footnote-5)** | **Good Practice** | **Assessment Step** | **Issue** **Cross-reference** | **Comment** |
| DSS06 | Changes made to master data are valid, complete, accurate and timely. | 1.1.1 Confirm that management executes transaction code MM04—Display Material Change Documents periodically and compares against source documents. Request a sample of source documents for evidence of comparison to inventory file updates. |  |  |
| DSS05DSS06 | Changes made to master data are valid, complete, accurate and timely. | 1.1.2 Review enterprise policies and process design specifications regarding access to maintain master data. Use transaction code SUIM to test user access to create (transaction code MM01), maintain (transaction code MM02) and delete (transaction code MM06) material master data.

|  |  |  |  |
| --- | --- | --- | --- |
| **Transaction(s)** | **Authorization Objects** | **Fields** | **Values** |
| MM01—Create Material & | M\_MATE\_MAR | ACTVT | 01 |
| M\_MATE\_STA | ACTVT | 01 |
| MM02—Change Material & | M\_MATE\_MAR | ACTVT | 02 |
| M\_MATE\_STA | ACTVT | 02 |
| MM06—Flag Material for Deletion | M\_MATE\_MAR | ACTVT | 06 |
| M\_MATE\_STA | ACTVT | 06 |

 |  |  |
| DSS06 | Changes made to master data are valid, complete, accurate and timely. | 1.1.3 Determine whether the configurable control settings address the risk pertaining to the validity, completeness and accuracy of master data and whether they have been set in accordance with management’s intentions. Use transaction code SPRO to display the IMG menu and follow the path as follows:* + - * Material types: Logistics—General 🡪 Material Master 🡪 Basic Settings 🡪 Material Types 🡪 Define Attributes of Material Types
			* Industry sector: Logistics—General 🡪 Material Master 🡪 Field Selection 🡪 Define Industry Sectors and Industry Sector-Specific Field Selection
			* Default price types: Execute transaction code OMW1—C RM-MAT MW Price Control, and determine whether default settings have been applied for the price control for material records.
 |  |  |
| DSS01DSS06 | Changes made to master data are valid, complete, accurate and timely. | 1.1.4 Determine whether appropriate management is reviewing the Materials List (transaction code MM60), or equivalent, by material type and confirm evidence of management’s review of the data on a periodic basis for accuracy and ongoing validity.Request evidence that management reviews periodically material master data (purchasing materials only) to verify whether the over delivery tolerance has been configured according to enterprise policies.Material master data tolerances are configured under the purchasing tab. Use transaction code MM01—Create Material or MM03—Display Material and review tolerance limits for a sample of material master records. Verify with management if the limits follow enterprise policies. |  |  |
| DSS06 | Inventory master data remains current and pertinent. | 1.2.1 Determine if the enterprise uses negative stocks for especial materials. Note: the standard SAP ERP settings do not allow negative stocks. The Neg. stocks allowed indicator has to be enabled to display the field in material master records. To configure negative stocks use transaction code SPRO to display the IMG menu and follow the path: Material Management🡪 Inventory Management and Physical Inventory🡪 Goods issue/transfer posting🡪 allow negative stocks (select plant and storage location).The indicator to allow negative stock must be enabled in the material master record of the specific materials for which negative stocks are allowed. Select a sample of material master records that allow negative stocks and confirm that management approved the configuration according to enterprise policies. |  |  |
| DSS05 | Settings or changes to the bill of materials or process order settlement rules are valid, complete, accurate and timely. | 1.3.1 Review enterprise policy and process design specifications regarding access to maintain BOM and process order settlement rules. Use transaction code SUIM—User Information System to test user access to create (transaction code CS01), change (transaction code CS02), make mass changes to (transaction code CS20), change single-layered work breakdown structure (WBS) BOM (transaction code CS72), change multilevel WBS BOM (transaction code CS75), and change multilevel WBS BOM using the browser (transaction code CSPB).

|  |  |  |  |
| --- | --- | --- | --- |
| **Transaction(s)** | **Authorization Objects** | **Fields** | **Values** |
| CS01—Create Material BOM | C\_AENR\_RV1 | ACTVT | 01 |
| C\_STUE\_BER | ACTVT | 01 |
| CS02—Change Material BOM | C\_STUE\_BER | ACTVT | 02 |
| C\_STUE\_WRK | ACTVT | 02 |
| CS20— Mass Change: Initial Screen | C\_STUE\_BER | ACTVT | 02 |
| CS72—Change WBS BOM | C\_STUE\_BER | ACTVT | 02 |
| C\_STUE\_WRK | ACTVT | 02 |
| C\_AENR\_BGR | ACTVT | 22 |
| CS75— Change multilevel WBS BOM | C\_STUE\_BER | ACTVT | 02 |
| C\_STUE\_WRK | ACTVT | 02 |
| C\_AENR\_BGR | ACTVT | 22 |

Test user access to transaction CSPB—Start WBS BOM Browser.Test user access to change settlement rules (user transaction code COR2 and follow the menu path: Logistic 🡪 Production—Process 🡪 Process Order 🡪 Process Order🡪 Change (enter the process order number and press **Enter**) 🡪Header🡪 Settlement Rule. |  |  |
| DSS06 | Settings or changes to the bill of materials or process order settlement rules are valid, complete, accurate and timely. | 1.3.2 Take a sample of BOM updates using transaction CS80— Change Documents for Material BOM and compare to authorized source documentation. |  |  |
| B-3.6a | Agree on the **process work products[[6]](#footnote-6)** (inputs and outputs as defined in the process practices description) that are expected to be present (process design).Assess to what extent the process work products are available. |  |  |
| Process **Master data maintenance** inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage. | Criteria: All listed work products should demonstrably exist and be used. |  |  |
| **Process Practice** | **Work Products** | **Assessment Step** |  |  |
| Master data maintenance | * Master data add/change/delete request forms
* Master data maintenance procedures
* Master data maintenance reports
* List of SAP users with master data access
 | Apply appropriate audit techniques to determine the existence and appropriate use of each work product. |  |  |
| B-3.7a | Agree on the **process capability level** to be achieved by the process. |  |  |
| *This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.* |  |  |
| **SAP ERP Inventory process: Raw materials management** |
| B-3.1b | Understand the **Process context.** |  |  |
| B-3.2b | Understand the **Process purpose.** |  |  |
| B-3.3b | Understand all process **stakeholders** and their roles: |  |  |
| **Raw materials management** stakeholders:  |  |  |
| B-3.4b | Understand the **Process goals** and related **metrics[[7]](#footnote-7)** and define expected Process values (criteria), and assess whether the Process goals are achieved, i.e., assess the effectiveness of the process. |  |  |
| The Process **Raw materials management** has three defined process goals. | The following activities can be performed to assess whether the goals are achieved. |  |  |
| **Process Goal** | **Related Metrics** | **Criteria/Expected Value** | **Assessment Step** |  |  |
| Inventory is salable, usable, and adequately safeguarded | * Slow moving inventory report
* Zero turns inventory report
* Number and value of miscellaneous adjustments
* Number and value of scrap adjustments
 | *Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.* | *In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.* |  |  |
| Raw materials are received and accepted only with valid purchase orders and are recorded accurately and in a timely manner | * Number and value of miscellaneous adjustments
* Number and value of scrap adjustments
 | *Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.* | *In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.* |  |  |
| Defective raw materials are returned to suppliers in a timely manner | * Number of material returns to vendor with average # of days since receipt of same PO line.
 | *Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.* | *In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.* |  |  |
| B-3.5b | Agree on suitable criteria to evaluate all processes in scope of the assurance engagement:Evaluate **Raw materials management** |  |  |
| **Reference****Process** | Raw materials management | Criteria: 2.1 Inventory is salable, usable and adequately safeguarded.2.2 Raw materials are received and accepted only with valid purchase orders and are recorded accurately and in a timely manner.2.3 Defective raw materials are returned to suppliers in a timely manner. |  |  |
| **Reference****Process Practices[[8]](#footnote-8)** | **Good Practice** | **Assessment Step** | **Issue** **Cross-reference** | **Comment** |
| APO11BAI04DSS01DSS06 | Inventory is salable, usable, and adequately safeguarded. | 2.1.1 Confirm that the MRP process takes into account stock on hand, forecast requirements, economic order quantities and back orders.  Confirm that data elements for MRP have been created as follows:* Material master
* Bill of materials
* Work centers
* Routings
* Demand management

Review the MRP configuration using transaction code SPRO to open the IMG menu and follow path: Material Management🡪Production Material 🡪Requirement Planning. Validate with management that the settings meet production specifications. |  |  |
| BAI04DSS06 | Inventory is salable, usable, and adequately safeguarded. | 2.1.2 Use transaction code MB5M— BBD/Prod. Date and ascertain the reason for an old stock being held (shelf life list).   Use transaction code MC50— Analysis of Dead Stock (i.e., stock quantity held in excess of production demands).Request evidence that management is reviewing this information on a regular basis. |  |  |
| APO11DSS01 | Inventory is salable, usable, and adequately safeguarded. | 2.1.3 Through interviews and observation, confirm that the quality department tests samples of raw materials, and rejected materials are adequately segregated into a separate quality assurance holding area and regularly monitored by the quality department personnel to ensure timely return to suppliers.  Obtain evidence that materials are returned to suppliers. |  |  |
| DSS01DSS06 | Inventory is salable, usable, and adequately safeguarded. | 2.1.4 Use transaction code MC46—Analysis of Slow-Moving Item to identify stock that has not been used for a certain period of time. Obtain evidence that management reviews of slow-turnover inventory and takes appropriate steps to address any unsalable materials. |  |  |
| DSS05DSS06 | Inventory is salable, usable, and adequately safeguarded. | 2.1.5 Inquire about the processes for shipping and receiving materials and obtain any documented procedures. Validate that personnel follows the process as described by management. Obtain evidence that all inbound and outbound movements are accompanied by the necessary documentation. |  |  |
| DSS05DSS06 | Inventory is salable, usable, and adequately safeguarded. | 2.1.6 Inquire about the processes for receiving and storing materials and obtain any documented procedures. Validate that personnel follows the process as described by management.Request to visit one or more areas designated to receive deliveries of raw materials and assess if physical security controls are in place to restrict access to authorized personnel only. Obtain evidence that physical security procedures are properly followed. |  |  |
| DSS05DSS06 | Inventory is salable, usable, and adequately safeguarded. | 2.1.7 Use testing technique 2.1.6 to test physical security controls for storage areas. |  |  |
| DSS01DSS06 | Raw materials are received and accepted only with valid purchase orders and are recorded accurately and in a timely manner. | 2.2.1 Review the reconciliation of the GR and/or IR accounts. Using transaction code MB5S—Display List of GR/IR Balances determine whether GR/IR account balances are periodically executed and reviewed. Check that there are appropriate procedures in place to investigate unmatched POs. In particular, long outstanding items should be followed up and cleared. Also check with the management and confirm that authorized individuals are given access to transaction code MR11—GR/IR account maintenance, which allows postings to GL (write off differences).  Use transaction code SUIM—User Information System to review the following authorization codes and activities:

|  |  |  |  |
| --- | --- | --- | --- |
| **Transaction(s)** | **Authorization Objects** | **Fields** | **Values** |
| MR11— GR/IR Account Maintenance | F\_BKPF\_BLA | ACTVT | 02 |
| F\_BKPF\_BUK | ACTVT | 02 |
| F\_BKPF\_GSB |  |  |

 |  |  |
| DSS01DSS06 | Raw materials are received and accepted only with valid purchase orders and are recorded accurately and in a timely manner. | 2.2.2 Use transaction code ME2M—Purchase Orders by Material to create a report of outstanding POs and ascertain from management whether there are reasons for any long-outstanding items on the report. Request evidence that management review periodically the list of open good receipt notes, POs and invoices and follows up on outstanding items as necessary. |  |  |
| APO11DSS01 | Raw materials are received and accepted only with valid purchase orders and are recorded accurately and in a timely manner. | 2.2.3 Request evidence that documents are marked as matched or paid, once matched or upon payment of the invoice, to prevent reuse. |  |  |
| DSS06 | Raw materials are received and accepted only with valid purchase orders and are recorded accurately and in a timely manner. | 2.2.4 Request evidence that management review periodically exception reports of good not received on time and that an investigation is initiated to identify problems. |  |  |
| DSS06 | Raw materials are received and accepted only with valid purchase orders and are recorded accurately and in a timely manner. | 2.2.5 Request evidence that goods received without a matching purchase order and overages are investigated before posting to the system and approving payment. Request evidence that management reviews periodically material master data (purchasing materials only) to verify whether the overdelivery tolerance has been configured according to enterprise policies. Use transaction code MM01—Create Material or MM03—Display Material and review tolerance limits for a sample of material master records. Verify with management whether the limits follow enterprise policies. |  |  |
| DSS05 | Raw materials are received and accepted only with valid purchase orders and are recorded accurately and in a timely manner. | 2.2.6 Use transaction code SUIM—User Information System to test user access to transactions for GR:* Post Goods Receipt for PO—MB01
* Goods movement—MIGO
* Post Goods Receipt for PO Unknown—MB0A
* Goods Movement (MM)—MIGO\_GO
* Goods Movement (Inventory Mgt.)—MIGO\_GI
* Transfer Posting—MIGO\_TR
* GR for Production Order—MB31
* Other Goods Receipts—MB1C
* Cancel Material Document—MBST

|  |  |  |  |
| --- | --- | --- | --- |
| **Transaction(s)** | **Authorization Objects** | **Fields** | **Values** |
| MB01— Post Goods Receipt for POMB0A— Post Goods Receipt for PO UnknownMIGO— Goods movementMIGO\_GO— Goods Movement (MM) | M\_MSEG\_BWE | ACTVT | 01 |
| M\_MSEG\_WWE | ACTVT | 01 |
| MB31— GR for Production Order | M\_RAHM\_BSA | ACTVT | 01 |
| M\_RAHM\_EKO | ACTVT | 01 |
| MB1C— Other Goods Receipts | M\_MSEG\_BWA | ACTVT | 01 |
| M\_MSEG\_BWE | ACTVT | 01 |
| M\_MSEG\_WWA | ACTVT | 01 |
| MBST— Cancel Material DocumentMIGO\_GI— Goods Movement (Inventory Mgt.)MIGO\_TR— Transfer Posting | M\_MSEG\_BMB | ACTVT | 01 |
| M\_MSEG\_WMB | ACTVT | 01 |

Test user access to high-risk movement types 561 through 566. These special movement types reflect the initial stock entry in the SAP ERP system at the time of conversion to the SAP ERP system. |  |  |
| DSS01 | Raw materials are received and accepted only with valid purchase orders and are recorded accurately and in a timely manner. | 2.2.7 Review the process for physical stock takes to confirm the complete, accurate, valid and timely recording of adjustments as a result of the stock-takes. Obtain evidence that count of physical inventory on a continuous basis is conducted by persons independent of day-to-day custody or recording of inventory. |  |  |
| DSS01DSS06 | Raw materials are received and accepted only with valid purchase orders and are recorded accurately and in a timely manner. | 2.2.8 Obtain evidence that physical inventory counts are reconciled to inventory records, and inventory records are reconciled to the GL (through transfer documents in the SAP ERP system). Validate that changes to the quantities of the inventory take place when they are moved (for sale to customer, rework, transfer, etc.). Movement type configuration dictates whether a material movement will update the material quantity. Review material quantity changes and/or movements and corresponding movement types via transaction MB51—Material Document List, which allows for the review of changes to several materials at the same time. Transaction code MB59— Material Doc. List allows for the search on multiple materials by a particular range of dates for material movement types starting with 5 (i.e., 5\*). Obtain a sample of inventory file updates using transaction code MB59 and compare the results to authorized source documentation. Inventory adjustment forms should be sequentially numbered and the sequence accounted for. |  |  |
| DSS06 | Raw materials are received and accepted only with valid purchase orders and are recorded accurately and in a timely manner. | 2.2.9 Obtain evidence that for raw materials and/or finished goods that are batch managed, there is an appropriate matching and accounting batch management strategy, including a periodic investigation on date expired, short expiration and defective batches, which are correctly matched with returned stock transactions.  |  |  |
| APO11DSS01 | Defective raw materials are returned to suppliers in a timely manner. | 2.3.1 Obtain evidence that rejected raw material is segregated in a specific holding area. Ascertain from management the movement type used to block processing and for returning rejected goods to suppliers (e.g., movement type 122).  |  |  |
| APO10DSS01 | Defective raw materials are returned to suppliers in a timely manner | 2.3.2 Execute transaction code MB51—Material Document List with the appropriate movement type. Determine whether there are any long outstanding materials pending return to suppliers and/or receipt of appropriate credits. Ascertain from management whether there are reasons for keeping the defective materials |  |  |
| B-3.6b | Agree on the **process work products[[9]](#footnote-9)** (inputs and outputs as defined in the process practices description) that are expected to be present (process design).Assess to what extent the process work products are available. |  |  |
| Process Raw materials management inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage. | Criteria: All listed work products should demonstrably exist and be used. |  |  |
| **Process Practice** | **Work Products** | **Assessment Step** |  |  |
| Raw materials management | * List of miscellaneous adjustments
* List of scrap adjustments
 | Apply appropriate audit techniques to determine the existence and appropriate use of each work product. |  |  |
| B-3.7b | Agree on the **process capability level** to be achieved by the process. |  |  |
| *This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.* |  |  |
| **SAP ERP Inventory process: Producing and costing inventory** |
| B-3.1c | Understand the **Process context.** |  |  |
| B-3.2c | Understand the **Process purpose.** |  |  |
| B-3.3c | Understand all process **stakeholders** and their roles: |  |  |
| **Producing and costing inventory** stakeholders:  |  |  |
| B-3.4c | Understand the **Process goals** and related **metrics[[10]](#footnote-10)** and define expected Process values (criteria), and assess whether the Process goals are achieved, i.e., assess the effectiveness of the process. |  |  |
| The Process **Producing and costing inventory** has one defined process goal. | The following activities can be performed to assess whether the goals are achieved. |  |  |
| **Process Goal** | **Related Metrics** | **Criteria/Expected Value** | **Assessment Step** |  |  |
| Transfers of materials to/from production, production costs, and defective products/scrap are valid and recorded accurately, completely and in the appropriate period | * Production order settlement completion rate
* Number of aged production orders
* Number of open production orders by month
 | *Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.* | *In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.* |  |  |
| B-3.5c | Agree on suitable criteria to evaluate all processes in scope of the assurance engagement.Evaluate **Producing and costing inventory** |  |  |
| **Reference****Process** | Producing and costing inventory | Criteria: 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. |  |  |
| **Reference****Process Practices[[11]](#footnote-11)** | **Good Practice** | **Assessment Step** | **Issue** **Cross-reference** | **Comment** |
| DSS01 | 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 receiving and transfer of materials and confirm that the previously described controls are in place and operating.  Obtain evidence that inventories and transfers received are compared to source documentation (e.g., pick list used to record movements of inventory in the financial records and recorded in the appropriate period). |  |  |
| APO11DSS01 | Transfers of materials to/from production, production costs and defective products/scrap are valid and recorded accurately, completely and in the appropriate period. | 3.1.2 Review the policy and procedures for the accounting of in-transit inventory and confirm that the described controls are in place and operating. Obtain evidence that management reviews the inventory-in-transit reports to ensure that amounts are cleared and reconciled. Confirm that inbound accounts net off outbound accounts for transfers from other facilities. |  |  |
| DSS01 | Transfers of materials to/from production, production costs and defective products/scrap are valid and recorded accurately, completely and in the appropriate period. | 3.1.3 Confirm that default price types have been established for all materials. Use transaction code OMW1— C RM-MAT MW Price Control, and determine whether default settings have been applied for the price control for material records. |  |  |
| APO11 | Transfers of materials to/from production, production costs and defective products/scrap are valid and recorded accurately, completely and in the appropriate period. | 3.1.4 Review records of scrapped and reworked items and checks whether such items have been correctly identified and properly recorded in the appropriate accounting period. |  |  |
| APO12DSS06 | Transfers of materials to/from production, production costs and defective products/scrap are valid and recorded accurately, completely and in the appropriate period. | 3.1.5 Test the tolerances for physical inventory differences: Use transaction code OMJ2— Maintain Phys.Inv.Tolrnce->Employee, compare defined tolerances to organizational policy and judge for reasonableness. **Note**: when transaction code OMJ2 is executed, the screen will provide two options for maintenance of inventory tolerance settings, either by physical inventory tolerance groups or by user name. If the company has adopted inventory tolerance control at the group level, execute transaction code OMJ2 and click physical inventory tolerance groups. If the tolerance has been set by specific users, select User Name. |  |  |
| DSS05 | Transfers of materials to/from production, production costs and defective products/scrap are valid and recorded accurately, completely and in the appropriate period. | 3.1.6 Review enterprise policy and process design specifications regarding access to maintain BOM and process order settlement rules. Use transaction code SUIM—User Information System to test user access to create (transaction code CS01), change (transaction code CS02), make mass changes to (transaction code CS20), change single layered work breakdown structure BOM (transaction code CS72), change multilevel WBS BOM (transaction code CS75), and change multilevel work breakdown structure BOM using the browser (transaction code CSPB).

|  |  |  |  |
| --- | --- | --- | --- |
| **Transaction(s)** | **Authorization Objects** | **Fields** | **Values** |
| CS01—Create Material BOM | C\_AENR\_RV1 | ACTVT | 01 |
| C\_STUE\_BER | ACTVT | 01 |
| CS02—Change Material BOM | C\_STUE\_BER | ACTVT | 02 |
| C\_STUE\_WRK | ACTVT | 02 |
| CS20— Mass Change: Initial Screen | C\_STUE\_BER | ACTVT | 02 |
| CS72—Change WBS BOM | C\_STUE\_BER | ACTVT | 02 |
| C\_STUE\_WRK | ACTVT | 02 |
| C\_AENR\_BGR | ACTVT | 22 |
| CS75— Change multilevel WBS BOM | C\_STUE\_BER | ACTVT | 02 |
| C\_STUE\_WRK | ACTVT | 02 |
| C\_AENR\_BGR | ACTVT | 22 |

Test user access to transaction CSPB—Start WBS BOM BrowserTest user access to change settlement rules (user transaction code COR2 and follow the menu path: Logistic 🡪 Production—Process 🡪 Process Order 🡪 Process Order 🡪Change (enter the process order number and press **Enter**) 🡪Header 🡪 Settlement Rule Take a sample of BOM updates using transaction CS80— Change Documents for Material BOM and compare to authorized source documentation. |  |  |
| DSS05 | Transfers of materials to/from production, production costs and defective products/scrap are valid and recorded accurately, completely and in the appropriate period. | 3.1.7 Use transaction code SUIM—User Information System to test user access to issue goods and to posting of transfers among plants:

|  |  |  |  |
| --- | --- | --- | --- |
| **Transaction(s)** | **Authorization Objects** | **Fields** | **Values** |
| MB1A—Goods Withdrawal, MB1B—Transfer Posting | M\_MSEG\_BWA | ACTVT | 01 |
| M\_MSEG\_WWA | ACTVT | 01 |

 |  |  |
| DSS05 | Transfers of materials to/from production, production costs and defective products/scrap are valid and recorded accurately, completely and in the appropriate period. | 3.1.8 Use transaction code SUIM—User Information System to test user access to create or change work centers.

|  |  |  |  |
| --- | --- | --- | --- |
| **Transaction(s)** | **Authorization Objects** | **Fields** | **Values** |
| CR01—Create Work Center | C\_ARPL\_WRK | ACTVT | 01 |
| CR02—Change Work Center | C\_ARPL\_WRK | ACTVT | 02 |

 |  |  |
| B-3.6c | Agree on the **process work products[[12]](#footnote-12)** (inputs and outputs as defined in the process practices description) that are expected to be present (process design).Assess to what extent the process work products are available. |  |  |
| Process **Producing and costing inventory** inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage. | Criteria: All listed work products should demonstrably exist and be used. |  |  |
| **Process Practice** | **Work Products** | **Assessment Step** |  |  |
| Producing and costing inventory | * Production order settlement log
 | Apply appropriate audit techniques to determine the existence and appropriate use of each work product. |  |  |
| B-3.7c | Agree on the **process capability level** to be achieved by the process. |  |  |
| *This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.* |  |  |
| **SAP ERP Inventory process: Handling and shipping finished goods** |
| B-3.1d | Understand the **Process context.** |  |  |
| B-3.2d | Understand the **Process purpose.** |  |  |
| B-3.3d | Understand all process **stakeholders** and their roles*.* |  |  |
| **Handling and shipping finished goods** stakeholders:  |  |  |
| B-3.4d | Understand the **Process goals** and related **metrics[[13]](#footnote-13)** and define expected Process values (criteria), and assess whether the Process goals are achieved, i.e., assess the effectiveness of the process. |  |  |
| The Process **Handling and shipping finished goods** has three defined process goals. | The following activities can be performed to assess whether the goals are achieved. |  |  |
| **Process Goal** | **Related Metrics** | **Criteria/Expected Value** | **Assessment Step** |  |  |
| Finished goods received from production are recorded completely and accurately in the appropriate period | * Number of open production orders by month
* Number of materials back-logged by month
 | *Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.* | *In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.* |  |  |
| Goods returned by customers are accepted in accordance with the organization’s policies | * Number of customer returns by month
* Number of customer returns without Return Authorization Numbers (RMAs)
 | *Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.* | *In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.* |  |  |
| Shipments are recorded accurately, in a timely manner and in theappropriate period | * Percentage of on-time shipping by storage location per week
 | *Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.* | *In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.* |  |  |
| B-3.5d | Agree on suitable criteria to evaluate all processes in scope of the assurance engagement.Evaluate **Handling and shipping finished goods** |  |  |
| **Reference****Process** | Handling and shipping finished goods | Criteria: 4.1 Finished goods received from production are recorded completely and accurately in the appropriate period.4.2 Goods returned by customers are accepted in accordance with the enterprise’s policies.4.3 Shipments are recorded accurately, in a timely manner and in the appropriate period. |  |  |
| **Reference** **Process Practices[[14]](#footnote-14)** | **Good Practice** | **Assessment Step** | **Issue Cross-reference** | **Comment** |
| APO12DSS01DSS06 | Finished goods received from production are recorded completely and accurately in the appropriate period. | 4.1.1 Test inventory stock-take procedures. Confirm that management executes transaction code MM04—Display Material Change Documents periodically and compares against source documents. Request a sample of source documents for evidence of comparison to inventory file updates. |  |  |
| DSS05DSS06 | Finished goods received from production are recorded completely and accurately in the appropriate period. | 4.1.2 Review enterprise policy and process design specifications regarding access to maintain BOM and process order settlement rules. Use transaction code SUIM—User Information System to test user access to create (transaction code CS01), change (transaction code CS02), make mass changes to (transaction code CS20), change single layered work breakdown structure BOM (transaction code CS72), change multilevel WBS BOM (transaction code CS75), and change multilevel work breakdown structure BOM using the browser (transaction code CSPB).

|  |  |  |  |
| --- | --- | --- | --- |
| **Transaction(s)** | **Authorization Objects** | **Fields** | **Values** |
| CS01—Create Material BOM | C\_AENR\_RV1 | ACTVT | 01 |
| C\_STUE\_BER | ACTVT | 01 |
| CS02—Change Material BOM | C\_STUE\_BER | ACTVT | 02 |
| C\_STUE\_WRK | ACTVT | 02 |
| CS20— Mass Change: Initial Screen | C\_STUE\_BER | ACTVT | 02 |
| CS72—Change WBS BOM | C\_STUE\_BER | ACTVT | 02 |
| C\_STUE\_WRK | ACTVT | 02 |
| C\_AENR\_BGR | ACTVT | 22 |
| CS75— Change multilevel WBS BOM | C\_STUE\_BER | ACTVT | 02 |
| C\_STUE\_WRK | ACTVT | 02 |
| C\_AENR\_BGR | ACTVT | 22 |

Test user access to transaction CSPB—Start WBS BOM Browser.Test user access to change settlement rules (user transaction code COR2 and follow the menu path: Logistic 🡪 Production—Process 🡪 Process Order 🡪 Process Order 🡪 Change (enter the process order number and press Enter) 🡪 Header 🡪 Settlement Rule.* Take a sample of BOM updates using transaction CS80— Change Documents for Material BOM and compare to authorized source documentation.
 |  |  |
| APO11 | Goods returned by customers are accepted in accordance with the enterprise’s policies. | 4.2.1Review the policies and procedures for receiving inventory back into the warehouse. Review some returns of inventory and ensure that they are supported with adequate documentation from the quality inspector. Ascertain from management the movement type used for goods returned from customers. Use transaction code MB51—Material Doc. List with the appropriate material movement type. Determine whether there are any long outstanding materials pending the return to inventory and/or provision of appropriate credits. |  |  |
| APO11 | Goods returned by customers are accepted in accordance with the enterprise’s policies. | 4.2.2 Obtain evidence that the QA team inspects the returned goods before a credit note can be issued. |  |  |
| DSS01DSS05 | Shipments are recorded accurately, in a timely manner and in the appropriate period. | 4.3.1 Use transaction code SUIM—User Information System to test user access to transfer stock among plants (transaction code LT04) or change outbound delivery (transaction code VL02N).

|  |  |  |  |
| --- | --- | --- | --- |
| **Transaction(s)** | **Authorization Objects** | **Fields** | **Values** |
| LT04—Create TO from TR | L\_TCODE | TCD | LT04 |
| VL02N—Change Outbound Delivery | V\_LIKP\_VST | ACTVT | 02 |

 |  |  |
| DSS05 | Shipments are recorded accurately, in a timely manner and in the appropriate period. | 4.3.2 Take a sample of the delivery due list and owed to customer report and test for evidence of management action. Review settings using transaction code OMWB— C MM-IV Autom. Acct. Assgt. (Simu.) to get the configuration screen for MM account assignments, use transaction key GBB and confirm that accounts assignments are set to valid COGS accounts. |  |  |
| DSS01 | Shipments are recorded accurately, in a timely manner and in the appropriate period. | 4.3.3 Review the policies and procedures for picking and shipping goods. Review a sample of shipments and ensure that they are supported with adequate documentation from the person matching physical quantity to order quantity. |  |  |
| DSS01 | Shipments are recorded accurately, in a timely manner and in the appropriate period. | 4.3.4 Request copies of the SAP ERP reports delivery due list and owed to customer report and confirm that these reports have been reviewed by the appropriate personnel to ensure timely shipment of goods. |  |  |
| DSS06 | Shipments are recorded accurately, in a timely manner and in the appropriate period. | 4.3.5 Use transaction key GBB and confirm that accounts assignments are set to valid COGS accounts. |  |  |
| B-3.6d | Agree on the **process work products[[15]](#footnote-15)** (inputs and outputs as defined in the process practices description) that are expected to be present (process design).Assess to what extent the process work products are available. |  |  |
| Handling and shipping finished goodsinputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage. | Criteria: All listed work products should demonstrably exist and be used. |  |  |
| **Process Practice** | **Work Products** | **Assessment Step** |  |  |
| Handling and shipping finished goods | * Past due delivery report
 | Apply appropriate audit techniques to determine the existence and appropriate use of each work product. |  |  |
| B-3.7d | Agree on the **process capability level** to be achieved by the process. |  |  |
| *This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.* |  |  |

| **Audit/Assurance Program for SAP ERP Inventory Business Cycle** |
| --- |
| **Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment****Organisational Structures** |
| **Ref.** | **Assurance Steps and Guidance** | **Issue****Cross-reference** | **Comment** |
| **B-4** | Obtain understanding of each **Organisational Structure** in scope and set suitable assessment criteria: For each **Organisational Structure** in scope (as determined in step A-3.3), additional information is collected and assessment criteria are defined. Assess the **Organisational Structure.** |  |  |
| **Organisational Structure:** **Warehouse** |
| B-4.1a | Understand the **Organisational Structure** context.*Identify and document all elements that can help to understand the context in which the* ***Financial accounting*** *organization has to operate, including:** *The overall organisation*
* *Management/process framework*
* *History of the role/structure*
* *Contribution of the Organisational Structure to achievement of goals*
 |  |  |
| B-4.2a | Understand all **stakeholders** of the **Organisational Structure**/function.*Determine through documentation review (policies, management communications, etc.) the key stakeholders of the* ***Financial accounting*** *organization.** *Incumbent of the role and/or members of the Organisational Structure*
* *Other key stakeholders affected by the decisions of the Organisational Structure/role*
 |  |  |
| B-4.3a | Understand the **goals** of the **Organisational Structure**, the related **metrics** and agree on expected values. Understand how these goals contribute to the achievement of the enterprise goals and IT-related goals. |  |  |
| **Organisational Structure Goal** | **Assessment Step** |  |  |
| Determine through interviews with key stakeholders and documentation review the goals of the **Warehouse** organization, i.e., **the decisions for which they are accountable[[16]](#footnote-16),[[17]](#footnote-17)**. | This step only applies if specific goals are defined. In that case, the assurance professional will use appropriate auditing techniques to:* Identify the decisions made by the Organisational Structure.
* Assess whether decisions are appropriately documented and communicated.
* Evaluate the decisions by, assessing whether:
	+ They have contributed to the achievement of the IT-related and enterprise goals as anticipated.
	+ Decisions are duly executed on a timely basis.
 |  |  |
| B-4.4a | Agree on the expected good practices for the **Organisational Structure** against which it will be assessed. Assess the **Organisational Structure design**, i.e., assess the extent to which expected **good practices** are applied. |  |  |
| **Good Practice** | **Criteria** | **Assessment Step** |  |  |
| Operating principles | * Operating principles are documented.
* Regular meetings take place as defined in operating principles.
* Meeting reports/minutes are available and are meaningful.
 | * Verify whether operating principles are appropriately documented.
* Verify that regular meetings take place as defined in the operating principles.
* Verify that meeting reports/minutes are available and are meaningful.
 |  |  |
| Composition | The Organisational Structure’s composition is balanced and complete, i.e., all required stakeholders are sufficiently represented. | Assess whether the Organisational Structure’s composition is balanced and complete, i.e., all required stakeholders are sufficiently represented. |  |  |
| Span of control | * The span of control of The Organisational Structure is defined.
* The span of control is adequate, i.e., the Organisational Structure has the right to make all decisions it should.
* The span of control is in line with the overall enterprise governance arrangements.
 | * Verify whether the span of control of the Organisational Structure is defined.
* Assess whether the span of control is adequate, i.e., the Organisational Structure has the right to make all decisions it should.
* Verify and assess whether the span of control is in line with the overall enterprise governance arrangements.
 |  |  |
| Level of authority/decision rights | * Decision rights of the Organisational Structure are defined and documented.
* Decision rights of the Organisational Structure are respected and complied with (also a culture/behaviour issue).
 | * Verify that decision rights of the Organisational Structure are defined and documented.
* Verify whether decision rights of the Organisational Structure are complied with and respected.
 |  |  |
| Delegation of authority | Delegation of authority is implemented in a meaningful way. | Verify whether delegation of authority is implemented in a meaningful way. |  |  |
| Escalation procedures | Escalation procedures are defined and applied. | Verify the existence and application of escalation procedures. |  |  |
| B-4.5a | Understand the life cycle and agree on expected values. Assess the extent to which the **Organisational Structure life cycle** is managed. |  |  |
| **Life-Cycle Element** | **Criteria** | **Assessment Step** |  |  |
| Mandate | * The Organisational Structure is formally established.
* The Organisational Structure has a clear, documented and well-understood mandate.
 | * Verify through interviews and observations that the Organisational Structure is formally established.
* Verify through interviews and observations that the Organisational Structure has a clear, documented and well understood mandate.
 |  |  |
| Monitoring | * The performance of the Organisational Structure and its members should be regularly monitored and evaluated by competent and independent assessors.
* The regular evaluations should result in the required continuous improvements to the Organisational Structure, either in its composition, mandate or any other parameter.
 | * Verify whether the performance of the Organisational Structure and its members is regularly monitored and evaluated by competent and independent assessors.
* Verify whether the regular evaluations have resulted in improvements to the Organisational Structure, in its composition, mandate or any other parameter.
 |  |  |
| **B-4.1 to B-4.5** | Repeat steps B-4.1 through B-4.5 for all remaining **Organisational structures** in scope. |  |  |
| Repeat the steps described above for the remaining Organisational structures: * Quality
* Shipping
* Financial accounting
* Tax department
* General accounting
* Treasury
 |  |  |

| **Audit/Assurance Program for SAP ERP Inventory Business Cycle** |
| --- |
| **Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment****Culture, Ethics and Behaviour** |
| **Ref.** | **Assurance Step and Guidance** | **Issue****Cross-reference** | **Comment** |
| **B-5** | Obtain understanding of the **Culture, Ethics and Behaviour** in scope.Assess Culture, Ethics and Behaviour. |  |  |
| **Culture, Ethics and Behaviour: Risk and compliance aware culture** |
| B-5.1a | Understand the **Culture, Ethics and Behaviour** **context**. * *What the overall corporate Culture is like*
* *Understand the interconnection with other enablers in scope:*
	+ *Identify roles and structures that could be affected by the Culture.*
* *Identify processes that could be affected by Culture, Ethics and Behaviour, including any processes in scope of the review.*
 |  |  |
| B-5.2a | Understand the major **stakeholders** of the **Culture, Ethics and Behaviour**: **Risk and compliance aware culture***Understand to whom the behaviour requirements will apply, i.e., understand who embodies the roles/structures expected to demonstrate the correct set of Behaviours. This is usually linked to the roles and Organisational Structures identified in scope.* |  |  |
| B-5.3a | Understand the **goals** for the **Culture, Ethics and Behaviour**, and the related **metrics** and agree on expected values. Assess whether the **Culture, Ethics and Behaviour goals** (outcomes) are achieved, i.e., assess the effectiveness of the Culture, Ethics and Behaviour. |  |  |
| In the context of **Risk and compliance aware culture**, the following **Culture, Ethics and Behaviour** are desired: | Culture and especially Behaviours are associated to individuals and the Organisational Structures of which they are a part, therefore, by using appropriate auditing techniques, the assurance professional will:* Identify individuals who must comply with the Behaviours under review.
* Identify the Organisational Structures involved.
* Assess whether desired Behaviours can be observed.
* Assess whether undesirable Behaviours are absent.

For a representative sample of individuals, perform the following assessment steps. |  |  |
| **Desired Behaviour (Culture, Ethics and Behaviour Goal)** | **Assessment Step** |  |  |
| The enterprise is aware of the compliance requirements it must abide |  |  |  |
| Employees understand their role in maintaining compliance |  |  |  |
| Identified risk are properly address |  |  |  |
| Controls are in place to ensure compliance with internal and external requirements |  |  |  |
| B-5.4a | Understand the life cycle stages of the **Culture, Ethics and Behaviour**, and agree on the relevant criteria.Assess to what extent the Culture, Ethics and Behaviour life cycle is managed. |  |  |
| (This aspect is already covered by the assessment of the good practices, hence no additional separate assurance steps are defined here.) |  |  |
| B-5.5a | Understand good practice when dealing with **Culture, Ethics and Behaviour**, and agree on relevant criteria. Assess the Culture, Ethics and Behaviour design, i.e., assess to what extent expected good practices are applied. |  |  |
| **Good Practice** | **Criteria** | **Assessment Step** |  |  |
| Communication, enforcement and rules | Existence and quality of the communication | Apply appropriate auditing techniques to assess whether the good practice is adequately applied, i.e., assessment criteria are met. |  |  |
| Incentives and rewards | Existence and application of appropriate rewards and incentives | Apply appropriate auditing techniques to assess whether the good practice is adequately applied, i.e., assessment criteria are met. |  |  |
| Awareness | Awareness of desired Behaviours | Apply appropriate auditing techniques to assess whether the good practice is adequately applied, i.e., assessment criteria are met. |  |  |
| **B-5.1 to B-5.5** | Repeat steps B-5.1 through B-5.5 for all remaining **Culture, Ethics and Behaviour** in scope. |  |  |
| Repeat the steps described above for the remaining Culture, Ethics and Behaviour: * Enabling of continuous improvement
* Accountability
* Discipline to follow instructions
 |  |  |

| **Audit/Assurance Program for SAP ERP Inventory Business Cycle** |
| --- |
| **Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment****Information Items** |
| **Ref.** | **Assurance Steps and Guidance** | **Issue****Cross-reference** | **Comment** |
| **B-6** | Obtain understanding of the **Information Items** in scope.Assess Information Items. |  |  |
| **Information Item: Data integrity procedures** |
| B-6.1a | Understand the Information item **context**:* *Where and when is it used?*
* *For what purpose is it used?*
* *Understand the connection with other enablers in scope, e.g.:*
	+ *Used by which processes?*
	+ *Which Organisational Structures are involved?*
	+ *Which services/applications are involved?*
 |  |  |
| B-6.2a | Understand the major **stakeholders** of the **Information item**.*Understand the stakeholders for the Information item, i.e., identify the:** *Information producer*
* *Information custodian*
* *Information consumer*

*Stakeholders should be at the appropriate organisational level.* |  |  |
| B-6.3a | Understand the major quality criteria for the Information item, the related metrics and agree on expected values. Assess whether the **Information item quality criteria** (outcomes) are achieved, i.e., assess the effectiveness of the Information item. |  |  |
| Leverage the COBIT 5 Information enabler model[[18]](#footnote-18) focusing on the quality goals description to select the most relevant Information quality criteria for the Information item at hand. Document expectations regarding information criteria. The COBIT 5 Information enabler model identifies 15 different quality criteria—although all of them are relevant, it is nonetheless possible and recommended to focus on a subset of the most important criteria for the Information item at hand.Mark the quality dimensions with a ‘✓’ that are deemed most important (key criteria), and by consequence will be assessed against the described criteria. | The assurance professional will, by using appropriate auditing techniques, verify all quality criteria in scope and assess whether the criteria are met. |  |  |
| **Quality Dimension** | **Key Criteria** | **Description** | **Assessment Step** |  |  |
| Accuracy | ✓ |  |  |  |  |
| Objectivity |  |  |  |  |  |
| Believability |  |  |  |  |  |
| Reputation |  |  |  |  |  |
| Relevancy | ✓ |  |  |  |  |
| Completeness | ✓ |  |  |  |  |
| Currency | ✓ |  |  |  |  |
| Amount of information | ✓ |  |  |  |  |
| Concise representation | ✓ |  |  |  |  |
| Consistent representation |  |  |  |  |  |
| Interpretability |  |  |  |  |  |
| Understandability | ✓ |  |  |  |  |
| Manipulation |  |  |  |  |  |
| Availability | ✓ |  |  |  |  |
| Restricted access | ✓ |  |  |  |  |
| B-6.4a | Understand the **life cycle** stages of the Information item, and agree on the relevant criteria. Assess to what extent the **Information item life cycle** is managed. |  |  |
| The life cycle of any Information item is managed through several business and IT-related processes. The scope of this review already includes a review of (IT-related) processes so this aspect does not need to be duplicated here.* When the Information item is internal to IT, the process review will have covered the life cycle aspects sufficiently.
* When the Information item also involves other stakeholders outside IT or other non-IT processes, some of the life cycle aspects need to be assessed.

Mark the life cycle stages with a ‘✓’ that are deemed most important (key criteria), and by consequence will be assessed against the described criteria. |  |  |
| **Life Cycle Stage** | **Key Criteria** | **Description** | **Assessment Step** |  |  |
| Plan | ✓ |  |  |  |  |
| Design | ✓ |  |  |  |  |
| Build/acquire | ✓ |  |  |  |  |
| Use/operate | ✓ |  |  |  |  |
| Evaluate/monitor | ✓ |  |  |  |  |
| Update/dispose | ✓ |  |  |  |  |
| B-6.5a | Understand important attributes of the Information item and expected values.Assess the **Information item design**, i.e., assess the extent to which expected **good practices** are applied. |  |  |
| Good practices for Information items are defined as a series of attributes for the Information item[[19]](#footnote-19). The assurance professional will, by using appropriate audit techniques, verify all attributes in scope and assess whether the attributes are adequately defined.Mark the attributes with a ‘✓’ that are deemed most important (key criteria), and by consequence will be assessed against the described criteria. |  |  |
| **Attribute** | **Key Criteria** | **Description** | **Assessment Step** |  |  |
| Physical |  |  |  |  |  |
| Empirical |  |  |  |  |  |
| Syntactic |  |  |  |  |  |
| Semantic |  |  |  |  |  |
| Pragmatic | ✓ |  |  |  |  |
| Social |  |  |  |  |  |
| **B-6.1 to B-6.5** | Repeat steps B-6.1 through B-6.5 for all remaining **Information items** in scope. |  |  |
| Repeat the steps described above for the remaining Information items: * Data classification guidelines
* Data security and control guidelines
* Assigned responsibilities for resource management
* Access logs
* Allocated roles and responsibilities
* Allocated levels of authority
* Allocated access rights
* Evidence or error correction and remediation
* Error reports and root cause analysis
* Retention requirements
* Record of transactions
* Training manuals
* Job aids
 |  |  |
| **Audit/Assurance Program for SAP ERP Inventory Business Cycle** |
| **Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment****Services, Infrastructures and Applications** |
| **Ref.** | **Assurance Steps and Guidance** | **Issue****Cross-reference** | **Comment** |
| **B-7** | Obtain understanding of the **Services, Infrastructure and Applications** in scope.Assess Services, Infrastructure and Applications. |  |  |
| **Services, Infrastructure and Applications: SAP ERP System** |
| B-7.1a | Understand the **Services, Infrastructure and Applications** context.*Understand the organisational and technological context of this service. Refer to step A-2.2 and A-2.3 and re-use that information to understand the significance of this Service, Infrastructure and Application.* |  |  |
| B-7.2a | Understand the major **stakeholders** of the **Services, Infrastructure and Applications**.*Understand who will be the major stakeholders of the service, i.e., the sponsor, provider and users. Stakeholders will include a number of organisational roles but could also link to Processes.* |  |  |
| B-7.3a | Understand the major **goals** for the **Services, Infrastructure and Applications**, the related **metrics** and agree on expected values. Assess whether the Services, Infrastructure and Applications goals (outcomes) are achieved, i.e., assess the effectiveness of the Services, Infrastructure and Applications. |  |  |
| **Goal** | **Criteria** | **Assessment Step** |  |  |
| Service description | * The Service is clearly described.
* Roles and responsibilities are clearly defined
* The Service is available to all potential stakeholders
 | * Verify that the Service exists and is clearly described.
* Verify that roles and responsibilities are clearly defined.
* Assess the quality of the Service description and of the Service offered.
* Verify the accessibility of the Service to all potential stakeholders.
 |  |  |
| Service level definition | Service levels are defined for : * Quality of the service deliverables
* Ease to request the service
* Timeliness
 | * Verify that the following aspects are dealt with in the Service level definitions:
	+ Quality of the Service deliverables
	+ Ease to request the service
	+ Timeliness
* Verify to what extent Service levels are achieved.
 |  |  |
| Contribution to related enablers, IT and enterprise goals | The Service contributes to the achievement of related enabler and IT-related and enterprise goals.  | Assess to what extent the Service contributes to the achievement of the related enabler goals and to the overall IT-related and enterprise goals. |  |  |
| B-7.4a | Understand good practice related to the Services, Infrastructure and Applications and expected values. Assess the **Services, Infrastructure and Applications** design, i.e., assess to what extent expected good practices are applied.*Leverage the description of Services, Infrastructure and Applications in the COBIT 5 framework[[20]](#footnote-20) to identify good practices related to Services, Infrastructure And Applications. In general the following practices need to be implemented:** *Buy/build decision needs to be taken.*
* *Use of the Service needs to be clear.*
 |  |  |
| **Good Practice** | **Criteria** | **Assessment Step** |  |  |
| Sourcing (buy/build) | A formal decision—based on a business case—needs to be taken regarding the sourcing of the Service. | * Verify that a formal decision—based on a business case—was taken regarding the sourcing of the Service.
* Verify the validity and quality of the business case.
* Verify that the sourcing decision has been duly executed.
 |  |  |
| Use | The use of the Service needs to be clear:* When it needs to be used and by whom
* The required compliance levels with the Service’s output
 | * Verify that the use of the Service is clear, i.e., it is known when and by whom the service needs to be used.
* Verify that actual use is in line with requirement above.
* Verify that the actual Service output is adequately used.
* Verify that Service levels are monitored and achieved.
 |  |  |
| **B-7.1 to B-7.4** | Repeat steps B-7.1 through B-7.4 for all remaining **Services, Infrastructure and Applications** in scope. |  |  |
| Repeat the steps described above for the remaining Services, Infrastructure and Applications: * Master data maintenance
* Change management
* SAP training
 |  |  |

| **Audit/Assurance Program for SAP ERP Inventory Business Cycle** |
| --- |
| **Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment****People, Skills and Competencies** |
| **Ref.** | **Assurance Steps and Guidance** | **Issue****Cross-reference** | **Comment** |
| **B-8** | Obtain understanding of the **People, Skills and Competencies** in scope.Assess People, Skills and Competencies. |  |  |
| **People, Skill and Competency: Proficiency using the SAP Inventory Module** |
| B-8.1a | Understand the **People, Skills and Competencies** context.*Understand the context of the Skill/Competency, i.e.,:** *Where and when is it used?*
* *For what purpose is it used?*
* *Understand the connection with other enablers in scope, e.g.:*
	+ *In which roles and structures is the Skill/Competency used? (See also B-4.1.)*

*Which behaviours are associated with the Skill/Competency?* |  |  |
| B-8.2a | Understand the major **stakeholders** for the People, Skills and Competencies.*Identify to whom in the organisation the skill requirement applies.* |  |  |
| B-8.3a | Understand the major **goals** for the **People, Skills and Competencies**, the related **metrics** and agree on expected values.Assess whether the **People, Skills and Competencies goals** (outcomes) are achieved, i.e., assess the effectiveness of the People, Skills and Competencies.For the People, Skills and Competencies: **Proficiency using the SAP Inventory Module**, the following goals and associated criteria can be addressed.  |  |  |
| **Goal** | **Criteria** | **Assessment Step** |  |  |
| Experience |  | Apply appropriate auditing techniques to assess whether the People, Skills and Competencies goals are adequately achieved, i.e., that assessment criteria are met. |  |  |
| Education |  |  |  |
| Qualification |  |  |  |
| Knowledge |  |  |  |
| Technical skills |  |  |  |
| Behavioural skills |  |  |  |
| Number of people with appropriate skill level  |  |  |  |
| B-8.4a | Understand the **life cycle** stages of the **People, Skills and Competencies**, and agree the relevant criteria.Assess to what extent the People, Skills and Competencies life cycle is managed. |  |  |
| For the People, Skills and Competencies at hand, the life cycle phases and associated criteria can be expressed in function of the process APO07. | For the People, Skills and Competencies at hand the assurance professional will perform the following assessment steps. |  |  |
| **Life Cycle Element** | **Criteria** | **Assessment Step** |  |  |
| Plan | Practice APO07.03 activity 1 (Define the required and currently available skills and competencies of internal and external resources to achieve enterprise, IT and process goals.) is implemented in relation to this skill. | Assess whether practice APO07.03 activity 1 is implemented in relation to this skill. |  |  |
| Design | Practice APO07.03 activity 2 (Provide formal career planning and professional development to encourage competency development, opportunities for personal advancement and reduced dependence on key individuals.) is implemented in relation to this skill.Practice APO07.03 activity 3 (Provide access to knowledge repositories to support the development of skills and competencies.) is implemented in relation to this skill. | Assess whether practice APO07.03 activity 2 is implemented in relation to this skill.Assess whether practice APO07.03 activity 3 is implemented in relation to this skill. |  |  |
| Build | Practice APO07.03 activity 4 (Identify gaps between required and available skills and develop action plans to address them on an individual and collective basis, such as training [technical and behavioural skills], recruitment, redeployment and changed sourcing strategies.) is implemented in relation to this skill. | Assess whether practice APO07.03 activity 4 is implemented in relation to this skill. |  |  |
| Operate | Practice APO07.03 activity 5 (Develop and deliver training programmes based on organisational and process requirements, including requirements for enterprise knowledge, internal control, ethical conduct and security.) is implemented in relation to this skill. | Assess whether practice APO07.03 activity 5 is implemented in relation to this skill. |  |  |
| Evaluate | Practice APO07.03 activity 6 (Conduct regular reviews to assess the evolution of the skills and competencies of the internal and external resources. Review succession planning.) is implemented in relation to this skill. | Assess whether practice APO07.03 activity 6 is implemented in relation to this skill. |  |  |
| Update/dispose | Practice APO07.03 activity 7 (Review training materials and programmes on a regular basis to ensure adequacy with respect to changing enterprise requirements and their impact on necessary knowledge, skills and abilities.) is implemented in relation to this skill. | Assess whether practice APO07.03 activity 7 is implemented in relation to this skill.  |  |  |
| B-8.5a | Understand good practice related to the **People, Skills and Competencies** and expected values.Assess the People, Skills and Competencies design, i.e., assess to what extent expected good practices are applied. |  |  |
| **Good Practice** | **Criteria** | **Assessment Step** |  |  |
| Skill set and Competencies are defined. | * Determine that an inventory of Skills and Competencies is maintained by organisational unit, job function and individual.
* Evaluate the relevance and the contribution of the Skills and Competencies to the achievement of the goals of the Organisational Structure, and by consequence, IT-related goals and enterprise goals.
* Evaluate the gap analysis between necessary portfolio of Skills and Competencies and current inventory of skills and capabilities.
 |  |  |  |
| Skill levels are defined. | * Assess the flexibility and performance of meeting Skills development to address identified gaps between necessary and current Skill levels.
* Assess the process for 360-degree performance evaluations.
 |  |  |  |
| B-8.1 to B-8.5 | Repeat steps B-8.1 through B-8.5 for all remaining **People, Skills and Competencies** in scope. |  |  |
| Repeat the steps described above for the remaining People, Skills and Competencies: * Proficiency using the SAP Materials Management Module
* Master data management skills
* Materials management skills and experience
* Proficiency running SAP reports
* Understanding of data classification policies
* Understanding of data integrity procedures
 |  |  |

|  |
| --- |
| **Audit/Assurance Program for SAP ERP Inventory Business Cycle** |
| **Phase C—Communicate the Results of the Assessment** |
| **Ref.** | **Assurance Step** | **Guidance** |
| **C-1** | **Document exceptions and gaps.** |  |
| C-1.1 | Understand and document weaknesses and their impact on the achievement of process goals. | * Illustrate the impact of enabler failures or weaknesses with numbers and scenarios of errors, inefficiencies and misuse.
* Clarify vulnerabilities, threats and missed opportunities that are likely to occur if enablers do not perform effectively.
 |
| C-1.2 | Understand and document weaknesses and their impact on enterprise goals. | * Illustrate what the weaknesses would affect (e.g., business goals and objectives, enterprise architecture elements, capabilities, resources). Relate the impact of not achieving the enabler goals to actual cases in the same industry and leverage industry benchmarks.
* Document the impact of actual enabler weaknesses in terms of bottom-line impact, integrity of financial reporting, hours lost in staff time, loss of sales, ability to manage and react to the market, customer and shareholder requirements, etc.
* Point out the consequence of noncompliance with regulatory requirements and contractual agreements.
* Measure the actual impact of disruptions and outages on business processes and objectives, and on customers (e.g., number, effort, downtime, customer satisfaction, cost).
 |
| **C-2** | **Communicate the work performed and findings.** |  |
| C-2.1 | Communicate the work performed. | * Communicate regularly to the stakeholders identified in A-1 on progress of the work performed.
 |
| C-2.2 | Communicate preliminary findings to the assurance engagement stakeholders defined in A-1. | * Document the impact (i.e., customer and financial impact) of errors that could have been caught by effective enablers.
* Measure and document the impact of rework (e.g., ratio of rework to normal work) as an efficiency measure affected by enabler weaknesses.
* Measure the actual business benefits and illustrate cost savings of effective enablers after the fact.
* Use benchmarking and survey results to compare the enterprise’s performance with others.
* Use extensive graphics to illustrate the issues.
* Inform the person responsible for the assurance activity about the preliminary findings and verify his/her correct understanding of those findings.
 |
| C-2.3 | Deliver a report (aligned with the terms of reference, scope and agreed-on reporting standards) that supports the results of the initiative and enables a clear focus on key issues and important actions. |  |

| **Inventory Business Cycle ICQ** |
| --- |
| **Control Objectives/Questions** | **Response** | **Comments** | **COBIT 5****References** |
| **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? |  |  |  |  | DSS06 |
| 1.1.2 Have the creation and maintenance of master data been assigned and restricted to a dedicated area within the enterprise that understands how they may affect organizational processes as well as the importance of timely changes? |  |  |  |  | DSS05 DSS06 |
| 1.1.3 Have configurable controls been designed into the process to maintain the integrity of master data? |  |  |  |  | DSS06 |
| 1.1.4 Does management periodically review master data to check that the overdelivery tolerance is different from zero percent or the unlimited delivery option is set? |  |  |  |  | DSS01 DSS06 |
| **1.2 Inventory master data remain current and pertinent.** |
| 1.2.1 Does management periodically review master data to check their accuracy? |  |  |  |  | DSS06 |
| **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? |  |  |  |  | DSS05 |
| 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? |  |  |  |  | DSS06 |
| **2. Raw Materials Management** |
| **2.1 Inventory is salable, usable and adequately safeguarded.** |
| 2.1.1 Are raw material requirements |  |  |  |  | APO11 |
| planned based on forecast | BAI04 |
| orders and production plans, and | DSS01 |
| does the system functionality | DSS06 |
| monitor and maintain inventory |
| levels in accordance with the |
| enterprise’s policies? |
| 2.1.2 Is the salability of finished goods and usability of raw materials (including shelf-life dates) assessed regularly during continuous inventory counts, and are any scrapped goods or raw materials appropriately approved? |  |  |  |  | BAI04 DSS06 |
| 2.1.3 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 holding area and regularly monitored by the quality department personnel to ensure timely return to suppliers? |  |  |  |  | APO11 DSS01 |
| 2.1.4 Does management review reports of slow-turnover inventory to ensure that it is still salable or usable? |  |  |  |  | DSS01 DSS06 |
| 2.1.5 Do goods inbound/outbound personnel monitor all incoming and outgoing vehicles and ensure that all goods leaving the premises are accompanied by duly completed documentation (e.g., intercompany stock transfer order, delivery docket or goods returned note)? |  |  |  |  | DSS05 DSS06 |
| 2.1.6 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? |  |  |  |  | DSS05 DSS06 |
| 2.1.7 Is inventory stored in properly secured (gates locked at night and premises alarmed), environmentally conditioned warehouse locations where access is restricted to authorized personnel? |  |  |  |  | DSS05 DSS06 |
| **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? |  |  |  |  | DSS01 DSS06 |
| 2.2.2 Are long-outstanding goods receipt notes, purchase orders and/or invoices investigated on a timely basis and accrued as appropriate? |  |  |  |  | DSS01 DSS06 |
| 2.2.3 Are documents canceled once or on payment of the invoice matched to prevent reuse? |  |  |  |  | APO11 DSS01 |
| 2.2.4 Does management review exception reports of goods not received on time for recorded purchases? |  |  |  |  | DSS06 |
| 2.2.5 When goods received are matched to open purchase orders, are receipts with no purchase orders, or those that exceed the purchase order quantity by more than an established amount, investigated? |  |  |  |  | DSS06 |
| 2.2.6 Is the ability to input, change or cancel goods received transactions restricted to authorized inbound logistics/raw materials personnel? |  |  |  |  | DSS05 |
| 2.2.7 Do persons independent ofday-to-day custody or recording of inventory count physical inventory on a continuous inventory basis? |  |  |  |  | DSS01 |
| 2.2.8 Are inventory counts reconciled to inventory records and inventory records reconciled to the GL? |  |  |  |  | DSS01 DSS06 |
| 2.2.9 Do raw materials/finished goods that are batch managed have a matching and accounting with an appropriate batch management strategy? |  |  |  |  | DSS06 |
| **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 holding area, and are they regularly monitored (assigned a movement type of 122) to ensure timely return to suppliers? |  |  |  |  | APO11 DSS01 |
| 2.3.2 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 credit is received in a timely manner? |  |  |  |  | APO10 DSS01 |
| **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 Are inventories received, including transfers, counted and compared to the pick list (thatis 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? |  |  |  |  | DSS01 |
| 3.1.2 Does management reconcile the inventory-in-transit accounts regularly, and do these accounts net off against other plants’ outgoing inventory-in-transit accounts? |  |  |  |  | APO11 DSS01 |
| 3.1.3 Is an appropriate costing method used for raw materials at purchase order price, and isthe raw materials costing rolled into finished goods on a monthly basis? |  |  |  |  | DSS01 |
| 3.1.4 Does the quality department, based on its 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? |  |  |  |  | APO11 |
| 3.1.5 Are tolerances for physical inventory differences configured to users from posting differences that exceed the tolerance? |  |  |  |  | APO12 DSS06 |
| 3.1.6 Is the ability to create or change bills of material restricted to authorized personnel? |  |  |  |  | DSS05 |
| 3.1.7 Is access to the material transfers and adjustments transactions appropriately restricted to authorized personnel? |  |  |  |  | DSS05 |
| 3.1.8 Is the ability to create or change work centers restricted to authorized personnel? |  |  |  |  | DSS05 |
| **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 ofday-to-day custody or recording of inventory count physical inventory on a continuous inventory basis? (Refer to master data integrity1.1.2.) |  |  |  |  | APO12 DSS01 DSS06 |
| 4.1.2 Is the changing of the settlement rules restricted to authorized users? (Refer to bill of materials integrity1.3.1.) |  |  |  |  | DSS05 DSS06 |
| **4.2 Goods returned by customers are accepted in accordance with the enterprise’s policies.** |
| 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? |  |  |  |  | APO11 |
| 4.2.2 Does the quality assurance team inspect the goods before a credit note can be issued? |  |  |  |  | APO11 |
| **4.3 Shipments are recorded accurately, in a timely manner 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 generatesan electronic (EDI) or manual invoice? |  |  |  |  | DSS01 DSS05 |
| 4.3.2 Do outbound logistics/finished goods personnel monitor all incoming and outgoing vehicles and ensure that all goods leaving the premises are accompanied by duly completed documentation (e.g., delivery docket or goods returned note)? |  |  |  |  | DSS05 |
| 4.3.3 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? |  |  |  |  | DSS01 |
| 4.3.4 Are the SAP ERP reports (delivery due list and owed-to-customer report) of open sales documents prepared and monitored to ensure timely shipment? |  |  |  |  | DSS01 |
| 4.3.5 Does the SAP ERP account assignment configuration ensure that amounts for shipped goods are posted to the appropriate COGS account? |  |  |  |  | DSS06 |

1. See *www.isaca.org/COBIT/Pages/Assurance-product-page.aspx* for more information on *COBIT 5 for Assurance*. [↑](#footnote-ref-1)
2. Because this is a business process audit/assurance program, several of the assurance steps associated with the COBIT 5 processes identified in step A-3.2 have been omitted. Audit/assurance programs for these processes can be found in the ISACA web site at *http://www.isaca.org/Knowledge-Center/Research/Pages/Audit-Assurance-Programs.aspx* and can be included in this audit/assurance program depending on the necessity to include them and on resources available. [↑](#footnote-ref-2)
3. For COBIT 5 processes, a set of goals and metrics are identified in *COBIT 5: Enabling Processes*. [↑](#footnote-ref-3)
4. For this audit/assurance program, COBIT 5 processes and their related activities are out of scope. Step B-3.5 describes the good practices and assurance steps for the SAP ERP Inventory processes in scope. [↑](#footnote-ref-4)
5. This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Inventory audit/assurance program. [↑](#footnote-ref-5)
6. For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in *COBIT 5: Enabling Processes*. [↑](#footnote-ref-6)
7. For COBIT 5 processes, a set of goals and metrics are identified in *COBIT 5: Enabling Processes*. [↑](#footnote-ref-7)
8. This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Inventory audit/assurance program. [↑](#footnote-ref-8)
9. For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in *COBIT 5: Enabling Processes*. [↑](#footnote-ref-9)
10. For COBIT 5 processes, a set of goals and metrics are identified in *COBIT 5: Enabling Processes*. [↑](#footnote-ref-10)
11. This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Inventory audit/assurance program. [↑](#footnote-ref-11)
12. For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in *COBIT 5: Enabling Processes*. [↑](#footnote-ref-12)
13. For COBIT 5 processes, a set of goals and metrics are identified in *COBIT 5: Enabling Processes*. [↑](#footnote-ref-13)
14. This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Inventory audit/assurance program. [↑](#footnote-ref-14)
15. For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in *COBIT 5: Enabling Processes*. [↑](#footnote-ref-15)
16. The RACI charts in *COBIT 5: Enabling Processes* can be leveraged as a starting point for the expected goals of a role or Organisational Structure. [↑](#footnote-ref-16)
17. The Organisational Structure/role as described may not exist under the same name in the enterprise; in that case, the closest Organisational Structure assuming the same responsibilities and accountability should be considered. [↑](#footnote-ref-17)
18. COBIT 5 framework, appendix G, p.81-84 [↑](#footnote-ref-18)
19. COBIT 5 framework, appendix G, p. 81-84 [↑](#footnote-ref-19)
20. COBIT 5 framework, appendix G, p.85-86 [↑](#footnote-ref-20)