The Assessor Examination

AX01
Scenario Booklet

This is a 2.5-hour objective test examination. This booklet contains the Project Scenario upon which this exam paper is based. All questions are contained within the *Question Booklet*.

Additional information is provided within this *Scenario Booklet* for a number of questions. Where reference should be made to additional information, this is clearly stated within the question to which it is relevant. All information provided within a question must only be applied to that question.

Each of the 8 questions is worth 10 marks, giving a maximum of 80 marks in the paper. The pass mark is 50% (40 marks). Within each question the syllabus area to which the question refers is clearly stated. The exam is to be taken with the support of the COBIT 5 Assessor Guide and the COBIT 5 Process Assessment Model (PAM) only, i.e. no material other than the *Question Booklet,* the *Scenario Booklet*, the *Answer Booklet* and the COBIT 5 Assessor Guide and the COBIT 5 PAM is to be used.

Candidate Number: .....

This is a blank page

Scenario (Note: The companies and people within the scenario are fictional)
Health Care Insurance

A major private international Health Care insurance company has its head office in the US and operates mainly in North America (Canada and the USA). It manages private health insurance for North American companies.

The key operations the company performs are:

- Managing online doctors, hospital and patient claims
- Managing private medical information
- HIPPA – Health Insurance Portability and Accountability ACT (which is about privacy and information security for covered organisations –mainly dealing with private medical records and insurance policies)
- All software and application management, including emergency changes is outsourced and managed by a third party company in Canada.
- Also outsourced is incident management and help desk to another company in the US.

Background and current issues:

- The organisation currently has issues around outsourcing performance to do with incident and problem management of third party vendors, and change management issues especially around emergency changes to the live production data base
- They also have access control issues to the live database for development and normal software upgrades.
    - Specifically emergency changes to live databases
- Outsourcing costs have been rising and the CFO and Chief of Business Operations are both very concerned
- Incidents have increased by 40% in the last year and the Chief of Business Operations would like to CIO to do a full assessment and review of the IT operations to see what needs to be improved or changed
- An internal and external audit report expressed concerns around the outsourcing contracts and potential access control issues to the live production database with changes not be properly authorised before updates have been made.
    - Specifically problems with monitoring service level agreements
    - Monitoring of external contracts
    - Procurement of IT services generally
- There is also concern on access control issues generally especially access to sensitive information and data by external third parties.
    - Specifically access privileges
    - Access by third party service providers to sensitive data.
- The external auditor obtained a statutory SOC (Service Organisation Control report – SSAE16) control report from each of the third party service providers on the effectiveness of key internal controls which did not find any significant deficiencies or material weaknesses
- The external audit partner and the Head of the audit committee have also expressed some concerns about the new health care act (HIPPA) in terms of data privacy and meeting the new security rule requirements which affect substantially the outsourced parties concerned.

Scenario continues on the next page

Scenario continued

A senior consultant and certified COBIT Assessor has been engaged by the enterprise. They have been contracted by the CIO to come in and do an independent assessment/evaluation of the company's IT operations and report back in 3 weeks' time. The CIO further elaborated that this will be an initial assessment to allow the company to embark upon a process improvement program.

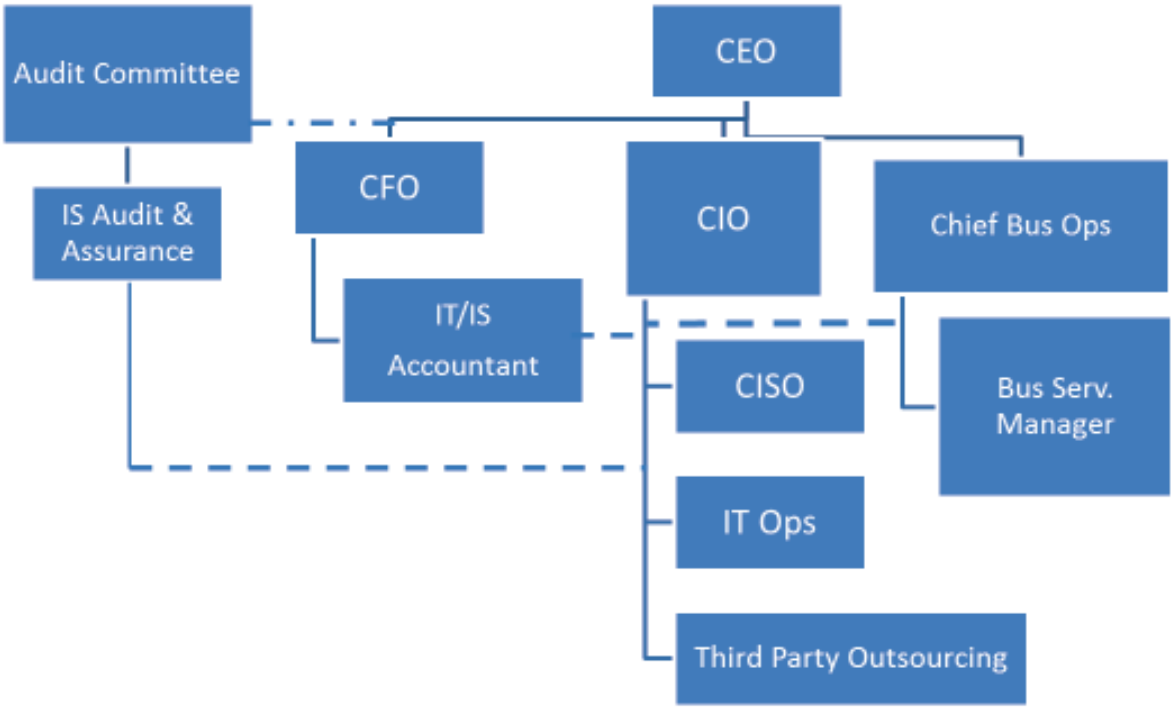
There is insufficient time to assess too many processes so scoping and prioritisation are very important as is an explanation and outline of the approach and the team selected to assist with the assessment.

This is NOT an audit of controls but an assessment of the process capabilities and making recommendations for improvement.

Scenario Continues on next Page

Scenario Continued

Organisational Structure of Roles in the Organisation affected by the assessment.



- The Chief of Business Operations is responsible for all health care processes.
- The Business Services Manager is responsible for working with IT to manage all service and operational level agreements and incidents
- An IT/IS Accountant is dedicated to IT operations
- The Chief Information Security officer reports to the CIO
- Audit, Assurance and Compliance have a dotted line to the CEO but report to an independent audit committee.
- There is a dedicated IS internal auditor.

End of scenario

Question 1: Roles, Responsibilities and Competences - Additional Information

Proposed Assessment Team

Roles	Proposed Assessment Team Roles	Reasons/rationale
Chief Executive Officer (CEO)	Not assigned	The CEO is from the insurance sector but has not worked in the private health insurance industry before. Was appointed to the CEO role six months ago and is committed to identifying the resources to help resolve the organisation's issues.
Chief Information Officer (CIO)	Sponsor	Although the CIO is not accountable for the business operation he has hired the consultant and will be responsible for implementing the changes required as a result of the findings.
Chief of Business Operations	Not assigned	Is responsible for all the business health care processes and managing the impact of the changes on the business. Is very concerned about the rising outsourcing costs and has asked the CIO to do a full assessment and review of the IT operations.
Consultant	Lead Assessor	From the specialist organisation contracted to do the COBIT assessment of the IT operations. Has undertaken many similar reviews and has extensive knowledge and expertise of COBIT.
Business Service Manager	Assessor	Is closely involved with managing the service level and operational level agreements (SLA/OLA) and the service contracts. Is in a good position to liaise with IT and the Business, in terms of who needs to be interviewed and access to the managers. Has never participated in an assessment before but is keen to take some training in COBIT5 and wants to learn.
IS/IT Internal Auditor	Coordinator	Has been trained a long time ago in a previous version of COBIT but has not got certification in the latest COBIT5 release. Knows the organisation's processes extremely well and can help with the process selection, data collection and validation.
Chief Information Security Officer (CISO)	Not assigned	Reports to the CIO Is responsible for resolving the issues surrounding the new Heath Care Act (HIPPA). Trained in the information security management system standard ISO27001 but has no experience of COBIT.

Question 3: Scope the Assessment - Additional Information

Mapping Enterprise processes to COBIT 5 PAM

Health Care Organisational Processes	COBIT 5 PAM Processes	Comments
IT Operations - DBA (Data Base Administration) - OLA & SLA management - Change Management	**Manage Service Agreements APO09 with the following key base practices:** - BP3 – Define & prepare service agreements - BP4 Monitor and report service levels - BP5 Review of Service agreements and contracts	The BSM works with the IT Operations department to develop and agree SLA's and OLA's for the delivery of IT services
	Manage Changes BAI06	
Manage Procurement - Manage supplier contracts - Monitor supplier performance - Supplier selection and vendor vetting - Manage Supplier SLA's	**Manage Suppliers APO10 with the following key base practices:** - BP1 Identify & evaluate supplier relationships and contracts. - Supplier selection - BP3 Manage Supplier relationships and contracts - BP4 Manage Supplier Risk - BP5 Monitor supplier performance and conformance	There is no supplier and risk assessment process in the organisational procurement process. The Business Services manager (BSM) works with the procurement team to ensure the appropriate inclusion of SLA's in contracts. But there is no Contract monitoring.
	Manage IT Operations DSS01 with the following key base practice: - BP2 - Manage Outsourced IT services	This COBIT process is also relevant to the Organisation's Procurement Processes for third party contracts as they relate to the provision of IT services.
IT Help Desk and Service Support - Record, Classify, prioritise issues and problems - Service request approval - Investigate and allocate incidents - Resolve and recover - Close requests and incidents - Monthly reporting	**Manage Service Requests and incidents DSS02**	
	Manage Problems DSS03	Problems are only managed as part of help desk incidents there are no dedicated procedures or process to look at problems separately, or in conjunction with incidents.

Additional Information continues on the next page

continued

IT Security Operations Includes: - Network security - Security Incidents monitoring - User Access and account management. - Malware & Virus Control - Security monitoring & reporting	**Manage Security DSS05 with the following key base practices:** - BP4 Manage user identity and logical access - BP2 Manage network and connectivity - BP3 Manage endpoint security - BP6 Manage sensitive documents and output devices - BP7 Monitor the infrastructure for security-related events	Issues with access controls, privileges and authority levels come up frequently. Concerns have been expressed by internal audit
	Manage Business Process Controls DSS06 with the following key base practice: - BP 3 Roles, responsibilities, access privileges and levels of authority	

Question 4: Plan an Assessment and Brief the teams and management - Additional Information

The Lead Assessor has written a memo to his team copied to the Sponsor outlining what he would like to include in a high-level plan for the healthcare organisation's assessment

The table below lists the key headings with sub topics:

ASSESSMENT PLAN – HIGH-LEVEL
1. Assessment Initiation activities. - Confirmation of the Sponsor - Purpose - Context - Assessment Team - Constraints - Roles & responsibilities - Assessment Class - Organisational units - Confirmation that the COBIT PAM will be used Comment: Decisions taken in the initiation phase are required to be included in the plan
2. Scoping - Mapping of organisational issues to COBIT processes - Mapping of COBIT processes selected to the organisation's processes. - Identification of the process instances Comment: Scoping is part of initiation but the Lead assessor has decided to make it a separate phase/topic area due to its importance and criticality for planning and execution.
3. Level of Effort - The type of assessment Class 1, 2 or 3 - The scope based on processes selected - Capability levels to be achieved.
4. Assessment Tools - Manual templates - Automated tools or template
5. Data Collection Strategy - What inputs are required - Will they use excel sheets or web-based tools
6. Detailed Risk Assessment
7. Detailed Schedule - Scheduling participant interviews and availability. - Scheduling required documents to be reviewed - Start and end times by phase headings o Data collection o Data validation o Process rating and capability determination o Assessment reporting.
8. Any Other Information - To be specified

Question 5: Data Collection - Additional Information

The Lead Assessor has produced the following data collection approach with recommended steps to allow the Assessment team to collect the appropriate data for evaluation:

Recommended Steps and Approach
The objective is to ensure that for each process in scope sufficient evidence exists to meet the assessment purpose. The following steps are recommended:
1. For Level 1, (termed the process dimension) select all base practices and work products in the process, as the entire process is being assessed under this assessment approach. For Level 2 – All Objective criteria, generic practices and generic work products must be looked at.
2. Evidence gathering includes: a. Interviewing the participants b. Observing or asking for the work products associated with the process. c. Observation of the systems and infrastructure used in the process to manage the practices and produce the selected work products. d. Use the work product inputs to support evidence of base practices being performed.
3. When looking at gathering evidence from Levels 2 to 5 termed the Capability Dimension, it may be appropriate to use some of the evidence gathered at process Level 1 (process dimension) as input into the Level's 2 to 5 data collection process.
4. Use prepared templates for the data collection, and record the information with the appropriate references to the organisation's processes and work products. Comments are also very valuable in explaining missing information and gaps, or areas that the organisation could improve.
5. Before going on to data validation ensure that the data collected is complete, i.e. that there is sufficient evidence collected to meet the assessment rating criteria.

Question 6: Data Validation - Additional Information

	GAPS & MISSING EVIDENCE		
Process ID	**Process Name**	**SUMMARY OF GAPS & MISSING EVIDENCE**	**Discussed with Process Owners**
APO09	Manage Service Agreements	WP4 is missing; services are catalogued but not assigned to a portfolio as portfolio management is not done. The CIO does not agree that this is necessary for their business so no further action was taken.	No
DSS03	Manage Problems	This process was not performed except as a small part of DSS02 where there existed criteria for problem registration. This was not considered sufficient by the assessment team. The Chief of Business Operations did not believe it was necessary to have a separate process; however the Lead Assessor emphasised that it didn't necessarily need a separate process. The key base practices and work products which were required as part of DSS03 should be in evidence.	Yes
BAIO6	Manage Changes	WP 4 Post implementation review of emergency changes was not deemed to be necessary by the IT Operations Manager. It is considered by the Assessment team to be a minor gap so this could get an F when the attribute rating process has been completed.	No
DSS02	Manage Service Requests and Incidents	All base practices were being done except that BP7 Status reporting was incomplete as it was missing a trends analysis. There were also a few work products not in evidence; WP 12 User confirmation of satisfactory resolution; WP14 Trends report. The Lead Assessor didn’t believe that this would be a major impact as the business requirements appeared to be met by the overall process being performed.	Yes
DSS06	Manage Business Process Controls	One work product missing a RACI chart was not produced in support of BP 3	Yes
DSS01	Manage IT Operations	The Base Practice BP2 Managed Outsourced Services and the associated work products were identified as a Key Process instance given the organisational issues with third party contracts. The entire process was being performed, however Back up Logs, WP2 were not being checked on a daily basis. This was deemed by the team to be important and would result probably in an F. Conversations with the Sponsor and management are needed to rectify and improve the process.	Yes

Question 7: Analyse and rate the process attributes and capability levels - Additional Information

Level 1 Evidence and Assessment (Part A)

The Assessment team has just completed assessing the following processes which relate to some of the issues being experienced by the organization at Level 1: BAI06 Manage Changes, APO09 Manage Service Agreements and DSS03 Manage Problems. The evidence provided for all three processes show some missing or incomplete base practices and work products.

The following tables summarise the key findings to assist the assessor team in assigning the correct ratings for the processes assessed.

Process ID **Process Name**	**BAI06** **Manage Changes**
Process Description	Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. This includes change standards and procedures, impact assessment, prioritisation and authorisation, emergency changes, tracking, reporting, closure and documentation.
Process Purpose	Enable fast and reliable delivery of change to the business and mitigation of the risks of negatively impacting the stability or integrity of the changed environment.

Base Practices	**Yes/No**	**Work Products Outcomes**	**Yes/No**	**Comments**
BA106 BP1 - Perform impact assessment; prioritise and authorise changes	No	BA106 WP1 Impact Assessments	No	Base practice is not being performed completely. Changes are being prioritised and authorised but there is no business impact analysis, which is deemed to be critical by the assessment team.
BA106 BP2 Manage Emergency Changes	Yes	BA106 WP2 Approved requests for change	Yes	
BA106 BP3 Track and Report change status	Yes	BA106 WP3 Change plan and schedule	Yes	
BA106 BP4 Close and document the changes	Yes	BA106 WP4 Post-implementation review of emergency changes	No	A post-implementation review of emergency changes is not done, but this is not deemed to be critical.
		BA106 WP5 Change request status reports	Yes	
		BA106 WP6 Change documentation	Yes	

Additional Information continues on next page

Additional Information continued

Process ID	**APO09**
Process Name	**Manage Service Agreements**
Process Description	Align IT-enabled services and service levels with enterprise needs and expectations, including identification, specification, design, publishing, agreement, and monitoring of IT services, service levels and performance indicators.
Process Purpose	Ensure that IT services and service levels meet current and future enterprise needs.

Base Practices	Yes/No	Work Products Outcomes	Yes/No	Comments
APO09-BP1 Identify IT Services	Yes			
APO09-BP2 Catalogue IT-related services	Yes			It is not referred to as a catalogue but a register, but it fulfils the same purpose.
APO09-BP3 Define and prepare service agreements	Yes			
APO09-BP4 Monitor and report service levels	Yes			
APO09-BP5 Review service agreements and contracts	Partly			Reviews done only once a year. There is a frequency issue which could be contributing to some of the problems with third party service providers.
		Identified gaps in IT services to the business	Yes	
		Definitions of standard services	Yes	
		Service definitions	Yes	
		Updated service portfolio	No	There is no portfolio of services by service type
		Service catalogues	Yes	
		SLAs	Yes	
		OLAs	Yes	
		Service level performance reports	Yes	
		Improvement action plans and remediations	Yes	
		Updated SLAs	Yes	

Additional Information continues on next page

Additional Information continued

Process ID	DSS03
Process Name	Manage Problems
Process Description	Identify and classify problems and their root causes and provide timely resolution to prevent recurring incidents. Provide recommendations for improvements
Process Purpose	Increase availability, improve service levels, reduce costs, and improve customer convenience and satisfaction by reducing the number of operational problems.

Base Practices	Yes/No	Work Products Outcomes	Yes/No	Comments
DSS03-BP1 Identify & Classify problems	No			
DSS03-BP2 Investigate and classify problems	Yes			Only incidents and requests are logged and investigated as problems
DSS03-BP3 Raise Known Errors	No			
DSS03-BP4 Resolve and close problems	Yes			Only incidents and requests are logged and investigated as problems
DSS03-BP5 Perform proactive problem management	No			
		Problem classification scheme	No	
		Problem status reports	Yes	As part of incident management and help desk
		Problem register	No	
		Root causes of problems	No	Root cause analysis not performed
		Problem resolution reports	Yes	As part of incident management and help desk
		Known-error records	No	
		Proposed solutions to known errors	No	
		Closed problem records	Yes	As part of incident management and help desk
		Communication of knowledge learned	No	
		Problem resolution monitoring reports	Yes	As part of incident management and help desk
		Identified sustainable solutions	No	

Question 7: Analyse and rate the process attributes and capability levels - Additional Information

Level 2 Evidence and Assessment (Part B)

The Assessment team has just completed assessing APO10 Manage Suppliers, DSS05 Manage Security Services and DSS06 Manage Business Process Controls at Level 2. These processes relate to some of the issues being experienced by the organization.

The following tables summarise the key findings using Generic reference ID's to assist the assessor team in assigning the correct ratings for the processes assessed.

Process ID **Process Name**	**APO10** **Manage Suppliers**
Process Description	Ensure that IT-related services provided by all types of suppliers meet enterprise requirements, including the selection of suppliers, management of relationships, management of contracts, and reviewing and monitoring of supplier performance for effectiveness and compliance.
Process Purpose	Minimise the risk associated with non-performing suppliers and ensure competitive pricing.

Capability Level	**Generic Practices (GPs)**	**Yes/No**	**Generic Work Products (GWPs)**	**Yes/No**	**Comments**
Level 2 Managed	GP 2.1.1	Yes	GWP 1.0 GWP2.0	Yes	
	GP 2.1.2	Yes	GWP 2.0 GWP 9.0	Yes	
	GP 2.1.3	No	GWP 4.0	No	Performance is not adjusted on a continuous basis. The procurement department does a yearly plan and sometimes will include adjustments based on a supplier and contract performance.
	GP 2.1.4	Yes	GWP 1.0 GWP 2.0	Yes	
	GP 2.1.5	Yes	GWP 2.0 GWP 9.0	Yes	
	GP 2.1.6	Yes	GWP 1.0 GWP 2.0	Yes No	There is no process communication plan
Capability Level	**Generic Practices (GPs)**	**Yes/No**	**Generic Work Products (GWPs)**	**Yes/No**	**Comments**
Level 2 Managed	GP 2.2.1	No	GWP 3.0	No	There is no process for defining, structuring or managing work products
	GP 2.2.2	No	GWP 1.0	No	
	GP 2.2.3	No	GWP 3.0	No	
	GP 2.2.4	No	GWP 4.0	No	

Additional Information continues on next page

Additional Information continued

Process ID	DSS05				
Process Name	Manage Security Services				
Process Description	Protect business information in order to maintain the level of information security risk acceptable to the enterprise establishing and maintaining information security roles and responsibilities, policies, standards, and procedures. Perform security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents.				
Process Purpose	Minimise the business impact of information security vulnerabilities and incidents.				
Capability Level	**Generic Practices (GPs)**	**Yes/No**	**Generic Work Products (GWPs)**	**Yes/No**	**Comments**
Level 2 Managed					
	GP 2.1.1	Yes	GWP 1.0 GWP 2.0	Yes	Information security is managed and performed well in this organisation
	GP 2.1.2	Yes	GWP 2.0 GWP 9.0	Yes	
	GP 2.1.3	Yes	GWP 4.0	Yes	
	GP 2.1.4	Yes	GWP 1.0 . GWP 2.0	Yes	
	GP 2.1.5	Yes	GWP 2.0 GWP 9.0	Yes	
	GP 2.1.6	Yes	GWP 1.0 GWP 2.0	Yes	
Capability Level	**Generic Practices (GPs)**	**Yes/No**	**Generic Work Products (GWPs)**	**Yes/No**	**Comments**
Level 2 Managed					
	GP 2.2.1	Yes	GWP 3.0	Yes	
	GP 2.2.2	Yes	GWP 1.0	Partially	Control documentation exist but there is no evidence of a Control Matrix; this is a minor improvement that will be recommended by the assessment team.
	GP 2.2.3	Yes	GWP 3.0	Yes	
	GP 2.2.4	Yes	GWP 4.0	Yes	

Additional Information continues on next page

Additional Information continued

Process ID	**DSS06**
Process Name	**Manage Business Process Controls**
Process Description	Define and maintain appropriate business process controls to ensure that information related to and processed by in-house or outsourced business processes satisfies all relevant information control requirements. Identify the relevant information control requirements and manage and operate adequate controls to ensure that information and information processing satisfy these requirements.
Process Purpose	Maintain information integrity and the security of information assets handled within business processes in the enterprise or outsourced.

Capability Level	Generic Practices (GPs)	Yes/No	Generic Work Products (GWPs)	Yes/No	Comments
Level 2 Managed					
	GP 2.1.1	Yes	GWP 1.0 GWP 2.0	Yes	
	GP 2.1.2	Yes	GWP 2.0 GWP 9.0	Yes	
	GP 2.1.3	Yes	GWP 4.0	Yes	
	GP 2.1.4	Yes	GWP 1.0 . GWP 2.0	Yes	
	GP 2.1.5	Yes	GWP 2.0 GWP 9.0	Yes	
	GP 2.1.6	Yes	GWP 1.0 GWP 2.0	Yes No	A communication plan is missing.
Capability Level	**Generic Practices (GPs)**	**Yes/No**	**Generic Work Products (GWPs)**	**Yes/No**	**Comments**
Level 2 Managed					Work Products are well managed
	GP 2.2.1	Yes	GWP 3.0	Yes	
	GP 2.2.2	Yes	GWP 1.0	Yes	
	GP 2.2.3	Yes	GWP 3.0	Yes	
	GP 2.2.4	Yes	GWP 4.0	Yes	

Question 7: Analyse and rate the process attributes and capability levels - Additional Information

Recommended Steps to rating the processes (Part C)

Steps Taken	Assessment Team's Reasoning
1. Documented Process for Process Attribute Rating: a. Assign specific conditions for each of the following rating scales: **b. Level 1** • N- Not achieved (There is very little or nothing of the process being performed) • P- Partially Achieved (A large part of the process is being performed but two key practices or three or more work products are missing) • L- Largely Achieved (Most of the process is being performed but there is at least one key practice missing or incomplete with at least one or two work products missing) • F- Fully Achieved (Almost all of the process is being achieved with what is missing being deemed to be a lower risk or being implemented so warrants an F) **c. Level's 2 – Level 5** • N- Not achieved (There is very little or nothing of the process being performed) • P- Partially Achieved (A large part of the process is being performed but two or more GP's and two or more GWP's are missing) • L- Largely Achieved (Most of the process is being performed but there are at least one key GP & one GWP are missing or incomplete) • F- Fully Achieved (All of the process is being achieved at Level 2 part 1 and part 2, with no missing GPs' and GWP's)	Timescales are limited for this assessment so the Assessment team decided to avoid using judgement with the ISO 15504 rating scales based on percentage ranges; e.g. N – Not achieving the process between 0% and 15%; They felt that it was inefficient to allow an assessor to use 'judgement' in arriving at his or her conclusions, which in turn would mean a consensus approach. This would be time-consuming and create many grey areas In addition, the Assessment team felt that it can influence assessors to make decisions based on mathematical calculations, which would distract him or her from looking at the substance of the evidence; not all missing practices and work products are equal in their business impact. The team decided to assign specific conditions for Level 1 separately to Levels 2 to 5 (see column 1 for the conditions). The rationale for a difference between Levels 1 and the other capability levels is that at Level 1 the specific attributes of the process is assessed as it is more detailed information in terms of evidentiary requirements. From Levels 2 to 5 an assessor is dealing at the capability dimension and not the process dimension and so is looking at evidence generically. Much less evidence will be looked at because it is generic for all processes. So the conditions are made stricter from Levels 2 to 5.

Additional Information continues on next page

2. Documented Process For Capability Level Assessment a. One Level at a time; i.e. all processes will be assessed at Level 1 before moving on to the next level regardless of if a process attained a F – Full rating and could be assessed immediately to a higher level. b. Report all Level 1 process results before moving to Level 2.	This approach eliminates the need to have an extra capability calculation step because, by doing one level at a time, the process result is the capability level being achieved. No Capability Level calculation is necessary with this recommended process. Because the decision was taken to assess one capability level at a time, (step 2), the Assessment team felt that there is no need to have a separate step for calculating the capability level. This is because an L – Largely or F – Fully is calculated by process in step 1, which means the process is achieving its purpose at Level 1 or achieving its attribute objectives from Level 2 onwards.
3. Assessment Rating results will be recorded in a process Profile register	This step allows the organisation to assign priorities to process improvement projects and set target levels for future assessments.

Question 8: Prepare and present assessment reports - Additional Information

The Sponsor has written to the Lead Assessor stating that he would like to have first view of the results before they are presented to any other party. The Assessment team think that the Sponsor's approach may cause issues so, after discussion with the team, the Lead Assessor has submitted a compromised proposal to the Sponsor.

The Sponsor's requirements for the reporting activities and the Lead Assessor's Proposal are given in the table below.

Step Number	**Sponsor's Requirements**	**Lead Assessor's Proposal.**
1	Prepare the assessment report, focussing on the implications of the assessment results.	Prepare the assessment report.
2	Then present the results to the Sponsor.	Present initial results to the Sponsor first but ask that he not share until the Lead assessor has had a chance to consult with the participants.
3	Assemble the assessment records for the Sponsor for retention and storage.	Present the assessment results to the participants.
4	Approval of the records by the Sponsor.	Assemble the assessment records for the Sponsor, (detailed data collection, validation and ratings information), to be able to arrange of retention and storage.
5	Present the results to the participants.	Approval of the records by the Sponsor.
6	Finalise the report and distribute to the relevant parties.	Finalise the report and distribute to the relevant parties.
7	Provide final feedback from the assessment.	Provide final feedback from the assessment. (Feedback provided to the participants as a means to improve the assessment process)

The Assessor Examination

AX01

Question Booklet

Candidate Number: .....

This is a blank page

Syllabus areas covered:

Question 1 - Roles, Responsibilities and Competences

Question 2 - Initiate an Assessment

Question 3 - Scope the Assessment

Question 4 - Plan an Assessment and Brief the teams and management

Question 5 - Data Collection

Question 6 - Data Validation

Question 7 - Analyse and rate the process attributes and capability levels

Question 8 - Prepare and present assessment reports

Question Number 1

Syllabus Area Roles, Responsibilities and Competences

Syllabus Area	Question Number	Part	Marks
Roles, Responsibilities and Competences	1	A	4

Answer the following questions on the roles of the assessment team and participants.

Remember to select 2 answers to each question.

1	Which **2** competences are required for a Lead Assessor?	
	A	Knowledge of ISO/IEC 15504-based assessments.
	B	The principal source of knowledge for the organisation processes to be assessed.
	C	To have undertaken at least two assessments as part of a team.
	D	To be able to provide attestation audit reports.
	E	Ability to accept results on behalf of the enterprise.
2	Which **2** competences are required for an Assessor?	
	A	Ability to understand and mediate between both the business and assessment needs.
	B	Personal attributes such as Leadership skills that contribute to effective performance.
	C	Experience of conducting at least two previous assessments.
	D	Knowledge of COBIT 5 and how to apply it to the processes being assessed.
	E	Skills in the application of the COBIT 5 PAM and how to apply it to the assessment.
3	For the purpose of conducting an assessment which **2** areas of knowledge are required for the process owners?	
	A	Project management and communication skills
	B	Knowledge of the organisation's work products.
	C	The COBIT 5 framework and the PAM.
	D	The assessment methodology and approach.
	E	Potential weaknesses of the business operations.
4	Which **2** responsibilities are assigned to the Sponsor?	
	A	Make decisions that support the assessment process.
	B	Ensure adequate interaction between the business and the Assessment team.
	C	Brief the process owners of the activities being assessed.
	D	Engage an assessment team and ensure adequate resources.
	E	Verify the extent of conformance of the assessment to ISO/IEC 15504 at the end of the assessment.

Syllabus Area	Question Number	Part	Marks
Roles, Responsibilities and Competences	1	B	6

Using the Organisational Structure given in the Scenario and the additional information provided for this question in the *Scenario Booklet, a*nswer the following question about the assessment team.

Lines 1 to 6 in the table below consist of an assertion statement and a reason statement. For each line identify the appropriate option, from options A to E, that applies. Each option can be used once, more than once or not at all.

Option	Assertion	Reason	
A	True	True	AND the reason explains the assertion
B	True	True	BUT the reason does not explain the assertion
C	True	False	
D	False	True	
E	False	False	

	Assertion		Reason
1	The CEO should verify that the Lead Assessor is a competent assessor.	BECAUSE	The Lead Assessor should have undertaken at least two assessments as part of a team.
2	The Chief of Business Operations should replace the CIO as the Sponsor.	BECAUSE	The Sponsor is responsible for ensuring that the assessment team have access to the relevant resources.
3	The consultant should NOT take the role of Lead Assessor.	BECAUSE	External Assessors should only be used for independent assessments.
4	The Business Service Manager is a suitable Assessor.	BECAUSE	An Assessor is responsible for making sure that resources are made available in a timely manner to meet the assessment schedule.
5	The IS/IT Internal Auditor would be better suited in an Assessor role on the assessment team.	BECAUSE	An Assessor should have an understanding of the processes to be assessed.
6	The Chief Information Security Officer should be included in the assessment team as an Assessor.	BECAUSE	An Assessor is responsible for collecting and validating the data required during the assessment.

Question Number 2

Syllabus Area Initiate an Assessment

Syllabus Area	Question Number	Part	Marks
Initiate an Assessment	2	A	4

Answer the following questions about the following Initiation Checklist.

INITIATION TASKS:
1. Define the context
2. Confirm the identity of the Sponsor
3. Define the assessment purpose
4. Submit a Pre-Assessment Questionnaire (PAQ)
5. Identify the ownership of the assessment records
6. Select the enterprise participants
7. Establish the assessment team
8. Submit Pre-Assessment Questionnaire
9. Confirm that the COBIT PAM will be used
10. Specify Constraints

1	Which important task is missing from the Checklist?	
	A	Agree the Assessment Class, whether Class One, Two or Three.
	B	Identify the need for and approve confidentiality agreements.
	C	Confirm the business participant's knowledge of the COBIT 5 PAM.
	D	Define the resources and schedule for the assessment.
2	Which type of constraint should be included in step 10 of the Checklist?	
	A	Control for information resulting from confidentiality agreements.
	B	Application of the products or services of the enterprise unit.
	C	Awareness of what is involved in an assessment process.
	D	Determining who will be the local coordinator (LAC) to manage the logistics.
3	Which factor in the enterprise unit should form part of step 1 in the Checklist?	
	A	Minimum, maximum or specific sample size for the assessment.
	B	Awareness of time and resource commitment necessary.
	C	The size, criticality and complexity of the products and services.
	D	The processes to be investigated within the enterprise unit.

Question continues on the next page

Question continued

4	Which task should be added to make the Checklist more complete?	
	A	Select the enterprise unit/s and their processes to be assessed.
	B	Define the responsibilities for all participants including the assessment team.
	C	Confirm the Sponsor's commitment to proceed with the assessment.
	D	Brief the organisational unit by explaining the purpose, scope and model.

Syllabus Area	Question Number	Part	Marks
Initiate an Assessment	2	B	2

Using the Scenario, answer the following questions about the Pre-assessment Questionnaire (PAQ) produced by the Lead Assessor and his team. The Questionnaire has been discussed with the Sponsor.

Proposed Pre-assessment Questionnaire:	
1.	What business units are affected by the issues?
2.	What products and services are undertaken by the business units?
3.	What are the detailed Issues and problems necessitating the process assessment?
4.	What type of assessment will be performed (Class 1, 2, 3)?
5.	What are management's expectations from the assessment assignment?
6.	What is the time and resource commitment necessary?

Remember to select 2 answers to each question.

1 The Sponsor feels that some items are missing for this organisation's assessment.

Which **2** areas are missing from the Questionnaire?

A	Establishing the assessment team.
B	Defining the tools to be used.
C	The detailed issues and problems.
D	Awareness of time and resources.
E	Mapping processes to COBIT 5.

2 The Sponsor feels also that there should be more questions added to the PAQ.

Which **2** additional questions could be added?

A	Which products and services would be thought of as critical to the business?
B	How does the assessment purpose align with the business goals?
C	Does each key Business Unit Manager understanding the approach to be used with the COBIT 5 Model?
D	Who should be the Coordinator?
E	What dates are the Business Services and IT Operations Managers available?

Syllabus Area	Question Number	Part	Marks
Initiate an Assessment	2	C	4

Answer the following question about assessment class. In a meeting with the Sponsor, key participants and senior management, the Consultant from the specialist organisation contracted to do the COBIT assessment explained that there were three assessment classes. He proposed that, given the organisation's issues and problems, a Class Three type of assessment should be adopted.

He outlined the following conditions to support his decision:

- A limited amount of processes could be assessed in three weeks; without a full scoping activity he had estimated about six key processes from the COBIT 5 PAM, based on the major issues the organization was facing
- He had also identified a few key 'Process Instances'
- The assessment scope, discussed with the Sponsor, was to be an internal assessment, performed by internal Assessors, trained and selected under the guidance of the external Lead Assessor
- The assessment would provide an initial basis for future process improvement projects.
- The assessment would provide the basis of sufficient conclusions to assist in identifying opportunities for process improvement
- The Sponsor wants to limit the scope to exclude organizational comparisons.

Lines 1 to 4 in the table below consist of an assertion statement and a reason statement. For each line identify the appropriate option, from options A to E, that applies. Each option can be used once, more than once or not at all.

Option	Assertion	Reason	
A	True	True	AND the reason explains the assertion
B	True	True	BUT the reason does not explain the assertion
C	True	False	
D	False	True	
E	False	False	

	Assertion		Reason
1	The assessment does NOT require an independent Lead Assessor if Class Type Three is adopted.	BECAUSE	An independent Lead Assessor is required only for Class Type One or Two assessments.
2	If Class Three is adopted, it is appropriate to select six process instances for each process for the assessment.	BECAUSE	The Class Type Three assessment has NO limit on the number of process instances.
3	A Class Type Two would be better to provide a sound and solid basis for process improvement for this assessment.	BECAUSE	The results of Class Type Two are well suited to providing a basis for an initial assessment at the commencement of an improvement programme.
4	A Class Type One would NOT be more suitable for the assessment project.	BECAUSE	For each process instance objective evidence is NOT required to be drawn for Class Type One.

Question Number 3

Syllabus Area Scope the Assessment

Syllabus Area	Question Number	Part	Marks
Scope the Assessment	3	A	5

Using the COBIT 5 PAM to verify your selection, answer the following question about the initial mapping of the organisation's processes to the COBIT PRM.

Column 1 shows a list of issues experienced by the Health Care Insurance company. Column 2 contains a selection of COBIT 5 processes from the COBIT PRM. For each issue in Column 1, select the process in Column 2 that it would map to. Each selection from Column 2 can be used once, more than once or not at all.

	Column 1	Column 2
1	Issue 1 - Incidents have increased by 40% in the last year, especially in the time it takes to resolve the incidents and recover the IT services. The number of service requests has also increased, overloading the help desk and incident management team.	A APO10 – Manage Suppliers B DSS05 – Manage Security Services C DSS02 – Manage Service Request & Incidents D APO08 - Manage Relationships E BAI06 – Manage Changes F APO09 – Manage Service Level Agreements G APO13 – Manage Security
2	Issue 2 - Audit has concerns about third party access to sensitive data, especially on specific SLA's and OLA's (Service Level and Operating Level Agreements) for security access requirements.	
3	Issue 3 – Third Party costs have been rising, especially around contracts and service delivery, with more compliance reviews on contracts being necessary.	
4	Issue 4 - Access control issues have increased, especially around sensitive enterprise documents as reported in the security events log.	
5	Issue 5 – Audit has concerns about compliance with statutory requirements on security and privacy rules, especially meeting HIPAA security access requirements.	

Syllabus Area	Question Number	Part	Marks
Scope the Assessment	3	B	5

Using the additional information provided for this question in the *Scenario Booklet*, and the COBIT 5 PAM, answer the following questions about the mapping of the COBIT 5 processes to the organisation's processes.

Decide whether the COBIT 5 processes mapped to the organisation's processes were appropriately selected and select the response that supports your decision.

1 There is NO dedicated process to managing service levels; the Business Service Manager must coordinate with two departments; Procurement for the management of supplier contracts and IT operations for Service Level Agreements (SLA's) and Operating Level Agreements (OLA's). The Assessment team selected APO09 Manage Service Agreements. Is this an appropriate selection?

A	No, because APO09 requires the organisation to have a process for monitoring SLA's in contracts.
B	No, because the organisation manages SLA's as part of IT Operations and Business Services.
C	Yes, because APO09 covers the entire IT operations and Business process, including procurement.
D	Yes, because APO09 relates exclusively to the service-level agreement process.

2 There is NO dedicated process or practice to manage outsourced suppliers; this is managed by the Procurement department from the perspective of contracts. The Assessment team selected APO10 Manage Suppliers and the management practice DSS01 BP2 Manage Outsourced IT Services.

Is this an appropriate selection?

A	No, because DSS01 BP2 is NOT a process relevant to the Procurement department.
B	No, because APO10 is sufficient to cover all of the procurement activities, making DSS01 BP2 redundant.
C	Yes, because in APO10, is best suited to managing supplier relationships, including third party contracts.
D	Yes, because DSS01 BP2 and APO10 are complimentary and necessary to be in scope for outsourced services.

3 Incidents are on the increase and seem to be a big problem for the organisation, with the help desk being overloaded with requests. DSS02 Manage Service Requests and Incidents and DSS03 Manage Problems have been selected.

Are these two processes appropriate to deal with the organisation's issues?

A	No, because the incidents relate to IT and DSS03 deals with business problems so it is NOT relevant to the assessment.
B	No, because DSS06 Manage Business Process Controls should be selected as well, as it contributes to incident resolution.
C	Yes, because DSS02 and DSS03 are necessary for the resolution of incidents and the management of service requests.
D	Yes, because both DSS02 and DSS03 are needed for the performance of proactive problem management.

Question continues on the next page

Question continued

4	Issues with access controls, privileges and authority levels come up frequently. Concerns have been expressed by internal audit about access to sensitive documents, with the possibility of the organisation being compromised in complying with statutory privacy and security requirements. DSS05 Manage Security Services was selected to be in scope. Is this an appropriate selection?	
	A	No, because the management of malware, worms, spyware and virus problems which relate to this issue should be included.
	B	No, because although DSS05 covers the security issues it does NOT cover all aspects, such as authority levels and privileges.
	C	Yes, because DSS05 deals specifically with access identity and logical access controls; this is sufficient to deal with the problems.
	D	Yes, because DSS05 has a practice for managing sensitive documents and output devices to deal with the security problems.
5	Access Controls are usually seen as an Information security issue, but the Lead Assessor explained to the Sponsor and Management team that good access controls were dependent on the definition of authority levels and user privileges matched to the right roles and responsibilities, which was a business process. So it was recommended that an additional process linked to a specific Base Practice should be included in the scope. DSS06 BP3 Roles, responsibilities, access privileges and authority levels was therefore selected by the assessment team. Is this an appropriate selection?	
	A	No, because DSS06 BP3 is mainly concerned with business process controls, roles and responsibilities, which are business issues.
	B	No, because DSS05 Manage Security Services contains the appropriate practices that are sufficient to resolve any access control issue.
	C	Yes, because DSS06 BP3 is the only relevant process when defining authority levels for access control.
	D	Yes, because security does NOT exist in isolation of the business roles and responsibilities, authority levels and privileges defined.

Question Number 4

Syllabus Area Plan an Assessment and Brief the teams and management

Syllabus Area	Question Number	Part	Marks
Plan an Assessment and Brief the teams and management	4	A	4

Using the additional information provided for this question in the *Scenario Booklet*, answer the following questions about the development of the assessment plan.

Remember to select 2 answers to each question.

1 Which **2** items of information are relevant when producing the Assessment Initiation activities section of the plan defined by the Lead Assessor?

A	Scheduling specific process base practices and work products required for the information security process to be reviewed by the Assessors.
B	The findings of this assessment will be used to judge the current process capabilities and make recommendations for future improvement.
C	The risk that the outsourced suppliers are uncooperative will be managed by specific briefings to third parties on the implications of non-compliance to the HIPPA Act.
D	The Change Control Coordinator is on annual leave during the interview period
E	Approval that the COBIT 5 PAM will be used for the assessment programme.

2 Which **2** items are relevant when producing the Scoping section of the plan defined by the Lead Assessor?

A	Mapping COBIT to the following Business processes; Incident management and outsourced suppliers.
B	The Sponsor indicated that the assessment must be completed within three weeks.
C	To meet the timescales, four Assessors must be recruited to work full time with the Lead Assessor.
D	The Business Services Manager is responsible for managing service level agreements with procurement and IT management.
E	Issue reports and change requests are key documents to be assessed.

Question continues on the next page

Question continued

3	Which **2** key issues are relevant when producing the Level of Effort section of the plan defined by the Lead Assessor?	
	A	How data will be collected, validated and managed throughout the assessment assignment for their incident and change management processes.
	B	The availability of the interviewees in the procurement department for reviewing the supplier contracts and service level agreements.
	C	The Lead Assessor would like to use an excel spread sheet template for data collection, analysis and evaluation for the outsourced services process.
	D	What evidence is required to be collected for their third party and contracts process, which depends upon which assessment class chosen.
	E	The assessment team identified the following organisation's processes; change management, and incident management to be included in the assessment.
4	Which **2** items are relevant when producing the Any Other Information section of the plan defined by the Lead Assessor?	
	A	Incident logs and service level agreements were identified as key process instances by the Lead Assessor.
	B	The Ownership of the assessment record and the person responsible for approving the assessor logs.
	C	A risk assessment that outlines potential impacts of changes to the assessment team, assessment scope.
	D	The criticality and complexity of their outsourced contracts was identified by the Sponsor as an important factor.
	E	It was agreed by the Sponsor and the Lead Assessor that the internal auditor would become one of the Assessors.

Syllabus Area	Question Number	Part	Marks
Plan an Assessment and Brief the teams and management	4	B	3

Answer the following question about planning the assessment.

Column 1 is a list of information used when planning the assessment. For each item of information in Column 1, indicate the order in which it should have been used according to the COBIT 5 Assessor Guide. Note that NOT all information required for planning is given. Match your answers to the options provided in Column 2.

	Column 1	Column 2
1	The Sponsor has identified that both the Business Service Manager and the IT Operations Manager will need to approve the assessment plan.	A First B Second C Third
2	A risk has been identified that the third party service providers may be uncooperative. These providers believe that they do NOT have any significant deficiencies or material weaknesses following an earlier statutory SOC (Service Organisation Control report – SSAE16) control report.	
3	It is required that a separate report is produced covering only the recommendations for improvements to the security processes necessary to achieve conformance to the new Health Care Act (HIPPA). This is for sending to the affected the outsourced parties.	

Syllabus Area	Question Number	Part	Marks
Plan an Assessment and Brief the teams and management	4	C	3

Answer the following question about briefing.

The Lead Assessor has called a briefing meeting for the assessment team, Sponsor, management team, Assessors and Participants. He has prepared a briefing note which has been approved by the Sponsor. Included in the briefing note is the following meeting agenda:

- Confirmation of the Units to be assessed.
- Confirmation of the purpose, scope, constraints.
- Confirmation of the processes identified to be in scope.
- Confirmation of the understanding of the approach and the COBIT model.
- Outline of the next steps and the timings.
- Outline of the prerequisites for data collection.

Lines 1 to 3 in the table below consist of an assertion statement and a reason statement. For each line identify the appropriate option, from options A to E, that applies. Each option can be used once, more than once or not at all.

Option	Assertion	Reason	
A	True	True	AND the reason explains the assertion
B	True	True	BUT the reason does not explain the assertion
C	True	False	
D	False	True	
E	False	False	

	Assertion		Reason
1	The assessment purpose and constraints do NOT need to be covered in the briefing meeting.	BECAUSE	The assessment participants do need to know what management have decided regarding purpose and resource constraints.
2	The briefing note provided by the Lead Assessor is NOT complete enough to provide a good basis for the meeting.	BECAUSE	A briefing meeting should provide a full understanding of the planning and the next steps for the assessment team.
3	There is NO need to include an understanding of the COBIT model in the briefing.	BECAUSE	The COBIT model will be covered by scoping and the mapping of detailed processes in the next phase.

Question Number 5

Syllabus Area Data Collection

Syllabus Area	Question Number	Part	Marks
Data Collection	5	A	2

Using the COBIT 5 PAM, answer the following questions about the instances of process performance.

The table below lists the *key process instances* to be included in the three processes selected by the Assessment Team for data collection and assessment. These process instances are based on the following organisation issues identified during the scoping phase:

- Audit concerns about access to sensitive data and privacy
- Access Control Issues
- Software and application updates and changes to live databases by third parties
- Incidents increased by 40% mainly with third party service provision
- Third Party contract costs increased.

Processes & Associated Process Instances
DSS05 MANAGE SECURITY
- Inventory of sensitive documents and devices
- Approved User Access Rights
- Access Privileges
APO09 MANAGE SERVICE AGREEMENTS
- None identified
BAI06 CHANGE MANAGEMENT
- Change Requests

*** Note: This does NOT mean that other work products will NOT be examined during the data collection phase. It means that the process instances identified are unique work products for the specific organisational issues and problems identified.*

Remember to select 2 answers to each question.

1	Select **2** 'process instances' that are important to the organisations issues, which would be necessary to be included in the data collection activities.	
	A	Service Level Agreements
	B	Security Incident Tickets
	C	Problem Status Reports
	D	Supplier Compliance Monitoring Review Results
	E	Service Level Performance Reports

Question continues on the next page

Question continued

2	Select **2** processes which are impacted by the process instance “Access Privileges”?	
	A	APO10 Manage Suppliers
	B	DSS05 Manage Security Services
	C	DSS06 Business Process Controls
	D	BAI06 Manage Changes
	E	DSS03 Manage Problems

Syllabus Area	Question Number	Part	Marks
Data Collection	5	B	3

Using the COBIT 5 PAM, answer the following questions about whether the recommended steps for data collection have been followed.

The Assessment Team has selected the process DSS05 Manage Security Services and there is a requirement to prepare data collection sheets for this process. To do this the team must select the correct Process Outcomes, Base Practices and Work Products (outputs) that are specific to the organisation's issues and concerns around information security. Note that while an entire process has to be assessed, there are certain key 'instances' that are critical that will receive more focus for the attribute rating phase later on. This step is therefore necessary to compliment the full selection of 'process instances'. The organisation's issues being addressed are:

- Privacy & Management of Sensitive Information
- User Access Controls
- Third Party Access to Sensitive Information

Remember to select 2 answers to each question.

1	Which **2** Process Outcomes should be included in the data collection process to address the highlighted organisational issues?	
	A	DSS05-O4
	B	DSS05-O3
	C	DSS05-O1
	D	DSS05-O5
	E	DSS05-O2
2	Which **2** Base Practices should be included in the data collection process to address the highlighted organisational issues?	
	A	DSS05-BP4
	B	DSS05-BP1
	C	DSS05-BP6
	D	DSS05-BP2
	E	DSS05-BP5
3	Which **2** Work Products (outputs only) should be included in the data collection process to address the highlighted organisational issues?	
	A	DSS05-WP6
	B	DSS05-WP13
	C	DSS05-WP1
	D	DSS05-WP4
	E	DSS05-WP11

Syllabus Area	Question Number	Part	Marks
Data Collection	5	C	5

Using the additional information provided for this question in the *Scenario Booklet*, answer the following question about the recommended data collection steps that have been customized by the Lead Assessor to fit the assessment being performed.

Lines 1 to 5 in the table below consist of an assertion statement and a reason statement. For each line identify the appropriate option, from options A to E, that applies. Each option can be used once, more than once or not at all.

Option	Assertion	Reason	
A	True	True	AND the reason explains the assertion
B	True	True	BUT the reason does not explain the assertion
C	True	False	
D	False	True	
E	False	False	

	Assertion		Reason
1	Step 1 should also consider the process instances when collecting evidence for the selected processes at Level 1.	BECAUSE	A general understanding of the process purpose and outcomes and base practices being undertaken is NOT necessary.
2	The evidence gathering in Step 2 should be reduced to only (a) interviewing participants and (b) asking for the work products associated with the process.	BECAUSE	It does NOT require a large volume of data to be collected for the selected processes to be assessed.
3	It is appropriate in Step 3 to use some of the Level 1 evidence when collecting data for Levels 2 to 5.	BECAUSE	Evidence at process capability Levels 2 to 5 may be more abstract than the evidence at process performance Level 1.
4	In Step 4, comments should NOT be recorded in the template to explain missing information.	BECAUSE	Data should be collected in a systematic manner using an explicitly identified data collection strategy and technique.
5	Step 5 is NOT required as part of data collection.	BECAUSE	Ensuring the data is sufficient to meet the scope will be covered under the data validation phase.

Question Number 6

Syllabus Area Data Validation

Syllabus Area	Question Number	Part	Marks
Data Validation	6	A	4

Using the COBIT 5 PAM, processes APO10, DSS02 and DSS06, answer the following questions about the data validation steps.

The Lead Assessor has asked his team to complete the following check list in order to validate the completeness of the data collected:

1. Check that all base practices have been reviewed for the selected processes
2. Verify that all the work product inputs supporting the base practices have been included
3. Verify that all work product outputs have been included
4. Verify that the process instances defined in the data collection phase have been identified, documented and included in the data collection sheets
5. Verify that the missing evidence is documented with appropriate comments and any other information to substantiate the evidence
6. Check that any assessment constraints in the collection phase were appropriately documented (e.g. unavailability of key participants and other resource and time constraints)
7. Verify that the assessment team has sufficient information together with the rating conditions defined to form the correct conclusions of the capability level/s achieved.

1	For APO10 the work product WP 7 is missing, but the base practice BP 4 appears to be present. What validation step applies?	
	A	Step 1
	B	Step 2
	C	Step 5
	D	Step 7
2	For DSS02 it is NOT clear if BP 2 (a key base practice) was properly documented; the data collection sheets says ‘Yes’ but there is no mention or reference to the input information that supports the base practice. What validation step applies?	
	A	Step 1
	B	Step 2
	C	Step 3
	D	Step 4

Question continues on the next page

Question continued

3	For DSS06 a process instance was defined as the ‘allocation of authority levels’, but the data collection sheet shows only that WP4 exists. What validation step applies?	
	A	Step 1
	B	Step 4
	C	Step 5
	D	Step 6
4	The Lead Assessor is unsure at this stage if all the appropriate information and evidence has been collected for APO10. What validation step applies?	
	A	Step 1
	B	Step 4
	C	Step 5
	D	Step 7

Syllabus Area	Question Number	Part	Marks
Data Validation	6	B	6

Using the additional information provided for this question in the *Scenario Booklet* and the COBIT 5 PAM, answer the following questions about data validation.

Decide whether the deficiencies of the data collected have been addressed appropriately, taking into consideration any problems with the availability of the data, and select the option that supports your decision.

1 For process APO09, were the gaps and missing evidence highlighted in the data collection phase appropriately addressed?

A	No, because the Sponsor does NOT agree that the missing work product WP4 is necessary for their organisation so NO further action was taken.
B	No, because the Lead Assessor failed to discuss and validate these issues with the process owners.
C	Yes, because the Sponsor was notified and accepted the findings and did NOT think the gaps significant.
D	Yes, because the missing work product is a minor gap and therefore would have very little bearing on the final rating.

2 For the process DSS03, there seems to be a misunderstanding with the Sponsor over whether missing base practices and work products should have a separate process for problem management.

Should the Lead Assessor call a meeting with the Sponsor, and Process owners to clarify the issues?

A	No, because the Sponsor, who is the Senior IT manager, feels it is covered in incident management and therefore NOT necessary.
B	No, because it is the job of the Sponsor to sort out communication issues and the Lead Assessor or his team should NOT get involved.
C	Yes, because the missing base practices and work products are quite significant to the business operations and have already been validated with the process owners.
D	Yes, because DSS03 should be a separate process as indicated by the Assessment team in the analysis of the missing evidence.

3 In the process BAI06, given the view of the IT Operations Manager should the Lead Assessor first discuss with the Sponsor before calling a joint meeting to clarify the issue?

A	No, because as process owner, the IT Operations Manager can confirm that it isn't necessary to have this work product in place.
B	No, because the assessment team has already considered that BAI06 could get an F – Fully rating.
C	Yes, because the missing work product is critical to the Manage Changes process, and is considered to be of major importance by the assessment team.
D	Yes, because the Sponsor must always be notified if there are significant problems or disputes with findings that come up in data validation.

Question continues on the next page

Question continued

4	For the process DSS02, the missing WP 12 on user confirmation concerns the Sponsor. The Lead Assessor and his team didn't feel that this was a major concern. Was the Lead Assessor correct?	
	A	No, because it is the Sponsor who, with the business Leadership at a later stage of the assessment decides on the implications of the assessment findings.
	B	No, because having an incomplete Base Practice BP 7 and a missing Work Product WP12 is deemed to be significant by the Lead Assessor.
	C	Yes, because the collection of the data was complete and all deficiencies were addressed in the validation phase.
	D	Yes, because the validation phase should be used to analyse the implications of missing evidence and make recommendations to the Sponsor and management.
5	The Chief of Business Operations expressed some concern with the process results of DSS06; the assessment was very brief in its analysis of the evidence gathered especially as this was a business process issue with impacts on IT and security. Was the Chief of Business Operations correct?	
	A	No, because the team had NO issues with this process apart from one small deficiency identified in the data collection sheets.
	B	No, because in the initiation phase the Lead Assessor would have outlined the process of data collection and validation.
	C	Yes, because DSS06 contains some very important base practices which could impact other processes in scope like DSS05.
	D	Yes, because DSS06 was mainly a business process with NO impact on IT processes or practices so extra analysis was unnecessary.
6	The Sponsor challenged the comments made about the results of the process DSS01 and felt that the missing Work Product was irrelevant, especially as the only reason the process was selected was because of the base practice BP2. Was the Sponsor correct?	
	A	No, because all the Work Products are equally as important to the entire process, so each one must be assessed and validated.
	B	No, because a key 'process instance' is identified for subsequent rating and a part process can NOT be assessed.
	C	Yes, because the missing Work Product is irrelevant to the organisational issues.
	D	Yes, because BP2 Managing Outsourcing Services is all that is required to match to the organisation's issues and problems.

Question Number 7

Syllabus Area Analyse and rate the process attributes and capability levels

Syllabus Area	Question Number	Part	Marks
Analyse and rate the process attributes and capability levels	7	A	3

Using the Level 1 Evidence and Assessment (Part A) given in the additional information provided for this question, answer the following question about rating the Level 1 assessment.

Column 1 is a list of the processes which were reviewed. Column 2 contains the rating scale to be used by the Assessment team. For each reviewed process in Column 1, select the appropriate rating from Column 2. Each selection from Column 2 can be used once, more than once or not at all.

	Column 1	Column 2
1	BAI06 Manage Changes.	A N- Not achieved (There is very little or nothing of the process being performed)
2	APO09 Manage Service Agreements.	B P- Partially Achieved (A large part of the process is being performed but two key practices or three or more work products are missing)
3	DSS03 Manage Problems.	C L- Largely Achieved (Most of the process is being performed but there is at least 1 key practice missing or incomplete with at least one or two work products missing)
		D F- Fully Achieved (Almost all of the process is being achieved with what is missing being deemed to be a lower risk or being implemented so warrants an F)

Syllabus Area	Question Number	Part	Marks
Analyse and rate the process attributes and capability levels	7	B	3

Using the Level 2 Evidence and Assessment (Part B) given in the additional information provided for this question and the COBIT 5 PAM, answer the following question about rating the Level 2 assessment.

It is assumed that all process were rated F – Fully at Level 1, as without this rating a process cannot be assessed at higher levels.

Column 1 is a list of the processes which were reviewed. Column 2 contains the rating scale to be used by the Assessment team. For each reviewed process in Column 1, select the appropriate rating from Column 2. Each selection from Column 2 can be used once, more than once or not at all.

	Column 1	Column 2
1	APO10 Manage Suppliers.	A N- Not Achieved (There is very little or nothing of the process being performed)
2	DSS05 Manage Security Services.	B P- Partially Achieved (A large part of the process is being performed but two or more GPs and two or more GWPs are missing)
3	DSS06 Manage Business Process Controls.	C L- Largely Achieved (Most of the process is being performed but there are at least one key GP & one GWP are missing or incomplete)
		D F- Fully Achieved (All of the process is being achieved at Level 2 part 1 and part 2, with no missing GPs and GWPs)

Syllabus Area	Question Number	Part	Marks
Analyse and rate the process attributes and capability levels	7	C	4

Using the Recommended Steps to rating the processes given in the additional information provided for this question in the *Scenario Booklet*, answer the following questions about the steps recommended by the Assessment team to rate the processes being assessed.

Decide whether the recommended steps proposed by the Assessment team are appropriate to be used and select the response that supports your decision.

1	Step 1 - Are the conditions outlined for Level 1 Attribute ratings appropriate?	
	A	No, because NO assessor judgement is catered for.
	B	No, because there is a deviation from the ISO 15504 requirements.
	C	Yes, because the approach makes it easier to meet the business priorities.
	D	Yes, because it is in strict alignment with the ISO 15504 requirements.
2	Step 1 - Are the conditions outlined for Level 2 to Level 5 attribute ratings appropriate?	
	A	No, because they should be consistent with the level 1 conditions.
	B	No, because NO consideration is given to looking at a % rating range when assessing the evidence.
	C	Yes, because Assessors are looking at more detailed and specific evidence from levels 2 to 5.
	D	Yes, because the evidentiary requirements are less, justifying stricter rating conditions.
3	Step 2 - Is the decision to assess one level at a time appropriate?	
	A	No, because the specific step dedicated to this in the Assessor Guide does NOT match the team's recommended steps.
	B	No, because, management would want to know what the process achieved at the next level if a process attains an F at a particular level.
	C	Yes, because it eliminates extra work by allowing the Assessors to focus on one level at a time.
	D	Yes, because from Levels 2 to 5 an Assessor is dealing with the process and NOT the capability dimension.
4	Step 3 - Is the decision to record all ratings and capability levels attained in a profile register appropriate?	
	A	No, because the COBIT Assessor Guide does NOT give guidance on process profiles.
	B	No, because a profile register does NOT help organisations assign priorities for process improvements.
	C	Yes, because future maturity assessments and internal audit control planning for the enterprise will benefit.
	D	Yes, because a record for future assessments will be created to allow for process prioritisation and target setting.

Question Number 8

Syllabus Area Prepare and present assessment reports

Syllabus Area	Question Number	Part	Marks
Prepare and present assessment reports	8	A	5

Answer the following questions about completing an Assessment Report.

The Lead Assessor has been asked to prepare the Assessment Report. Each of the following 5 questions contain **true statements** about what is included in the report based on the assessment scenario.

Remember to select 2 answers to each question.

1	Which **2** statements should be recorded under the Purpose of Assessment Statement heading?	
	A	The determination of the capability level attained for the IT-related processes identified; APO09/10, BAI06, and DSS01/02/03/05/06 and their possible impacts.
	B	The summary of the results with capability level attained and their consequences for the processes APO09/10, BAI06, DSS01/02/03/05/06.
	C	To be able to identify good practices that might be implemented to improve the organisation's processes APO09/10, BAI06, and DSS01/02/03/05/06.
	D	The detailed mappings of the organisation's issues and problems to the COBIT processes APO09/10, BAI06, DSS01/02/03/05/06 selected for the assessment.
	E	The Sponsor had a requirement that the assessment was to be completed within three weeks.
2	Which **2** statements should be recorded under the Scope of the Assessment heading?	
	A	The assessment used an approach that assigned specific conditions for Level 1 separately to Levels 2 to 5.
	B	The processes which were assessed were BAI06, APO09, DSS03.
	C	The assessment has been given three weeks for evaluation, with the report due at the end of the financial year.
	D	The process selection was based on the organisation's issues and problems highlighted in the initiation and scoping phases.
	E	DSS03 Manage Problems was the worst performing process, achieving an N - Not Achieved rating.

Question continues on the next page

Question continued

3	Which **2** statements should be recorded under the Assessment Constraints heading?	
	A	The briefing must be completed within three days of the commencement of the assessment, to enable enough time for interviews.
	B	The CISO has been appointed by the Sponsor to be the custodian of the assessment record and owner of the assessment deliverables.
	C	The following specific processes will be reviewed; APO09, APO10, BAI06, DSS01/02/03/05/06, because they relate to the outsourcing and security issues being experienced.
	D	The internal auditor will be responsible for scheduling all interviews and arranging for the availability of the review documents for the Assessment team.
	E	'Service Level agreements' and 'Incident Logs' were identified as the key process instances that will affect the attribute and capability ratings for the selected processes.
4	Which **2** statements should be recorded under the Summary of Approach heading?	
	A	APO10 Manage Suppliers was performing the process at Level 1 with an L – Largely Achieved rating, which is a normal rating in most enterprises.
	B	The COBIT 5 Assessment programme, which includes a PAM and Assessor Guide were used for the assessment.
	C	It was agreed that the Chief Business Officer would be the Sponsor and the Business Services Manager would be the Coordinator.
	D	It was determined and agreed in the initiation phase that this assessment was a Class 2 assessment.
	E	The Internal auditor and the Lead Assessor would be responsible for all interviews of the participants, and reviewing the selected work products and base practices.
5	Which **2** statements should be recorded under the Detailed Findings heading?	
	A	The purpose of assessing the Procurement, IT Operations, and Information security units was to determine the process capability levels of the selected processes.
	B	The summary chart shows that APO09 attained a capability level of L - Largely Achieved, and DSS03 a level of N - Not Achieved.
	C	DSS02 was an important process to be selected because it dealt with one of the key issues and problems around IT incident management.
	D	The risk of APO09 SLA's attaining an L – Largely Achieved rating is classed as major because the impact to the organisation of third party contracts NOT performing is significant.
	E	DSS03 failed to perform because of missing base practices and work products and therefore the process outcomes were NOT achieved.

Syllabus Area	Question Number	Part	Marks
Prepare and present assessment reports	8	B	5

Using the additional information provided for this question in the *Scenario Booklet*, answer the following question about the steps required to produce the Assessment report.

Lines 1 to 5 in the table below consist of an assertion statement and a reason statement. For each line identify the appropriate option, from options A to E, that applies. Each option can be used once, more than once or not at all.

Option	Assertion	Reason	
A	True	True	AND the reason explains the assertion
B	True	True	BUT the reason does not explain the assertion
C	True	False	
D	False	True	
E	False	False	

	Assertion		Reason
1	In Step 1 of the Sponsor's requirements, the implications of the assessment results should NOT be included in the report.	BECAUSE	The organisation is responsible for assessing the risks associated with the capability level attained for each process.
2	It is likely to affect the commitment of staff to future assessments if the Sponsor sees the results before the participants.	BECAUSE	Buy-in from the team is needed to ensure that all inputs and outcomes are properly addressed according to the data found.
3	The revised order of the recommended steps for Steps 1 to 3, as proposed by the Lead Assessor, is an appropriate compromise to offer the Sponsor.	BECAUSE	It is the responsibility of the Lead Assessor to confirm receipt of the assessment result.
4	In the Lead Assessor's Proposal, the report should be finalised and distributed before the assessment records are assembled for the Sponsor.	BECAUSE	It is recommended that the Assessment report is finalised and distributed after the assessment results have been presented.
5	Step 6 of the Lead Assessor's Proposal should include distributing the report to the Audit Committee.	BECAUSE	An Assessment report is a good indicator of the effectiveness of the process or its internal controls.