SECURE DATABASES

UNIT CODE: SEC/OS/CS/CR/05/6/A

UNIT DESCRIPTION

This unit covers the competencies required to secure databases. Competencies includes; identifying types of databases, identifying database threats and vulnerabilities, installing database patches, installing database security management system, monitoring database security, monitoring access control and managing database backups.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT These describe the key outcomes which make up workplace function.	**PERFORMANCE CRITERIA** These are assessable statements which specify the required level of performance for each of the elements. ***(Bold and italicised terms are elaborated in the Range)***
1. Identify types of databases	1.1 Database type is identified as per the types of data it holds 1.2 Database is established as per the amount of data it holds 1.3 Database is classified as per its distribution 1.4 Database type is determined in line with the number of users 1.5 Database is identified as per its operational model 1.6 Cost evaluation is adhered to in database type identification
2. Identify database threats and vulnerabilities	2.1 Database tests are performed as per the manufacturers manual 2.2 Security vulnerabilities and exposures updates are assessed as per the standard operation procedures 2.3 Database is checked for misconfiguration as per the manufacturers guide
3. Install databases patches	3.1 Required patches are identified and acquired as per manufacturers guidelines 3.2 Required patches are verified as per the manufacture's guidelines 3.3 Database patches are deployed in a test environment as per the organization quality assurance policy. 3.4 Database patches are monitored as per the ICT policy 3.5 Database patches are deployed in the production

ELEMENT These describe the key outcomes which make up workplace function.	PERFORMANCE CRITERIA These are assessable statements which specify the required level of performance for each of the elements. ***(Bold and italicised terms are elaborated in the Range)***
	environment as per the organization policy.
4. Install database security management systems	4.1 Type of database security management system is established as per the client's requirements 4.2 Security management system is established in line with the deployment model 4.3 Hardware sizing is performed in line with database to be secured 4.4 Security management system is installed and configured according to manufacturer's manual 4.5 Security management system is verified as per the guidelines in database security management system set up. 4.6 System integration is performed as per the manufacturers manual and clients requirement
5. Monitor database security	5.1 Logs are collected and analysed as per the standard operating procedure 5.2 Failed log in attempts are monitored as per system operation 5.3 Database firewall is configured as per the database expected operation 5.4 Remote access is monitored as per database operation 5.5 Odd hours database access monitored as per the its operation 5.6 Change in user access patterns is monitored in with the operation of the database 5.7 Random change in size of the database is monitored as per its normal size. 5.8 File configuration changes are monitored as per database operation.
6. Manage access control	6.1 Failed log in attempts are identified as per the system operation 6.2 Privilege account abuse is checked as per the access control policy 6.3 Users access control is managed in line with the least privileged principle 6.4 Active directory rules are adhered to in database access

ELEMENT These describe the key outcomes which make up workplace function.	PERFORMANCE CRITERIA These are assessable statements which specify the required level of performance for each of the elements. ***(Bold and italicised terms are elaborated in the Range)***
	6.5 Database is accessed by allowed devices as per the organizations policy 6.6 Obfuscation is adhered to in database access 6.7 Database auditing system is established as per the nature of the data to be secured
7. Manage database backups	7.1 Automatic backups are scheduled as per the ICT policy and regulations 7.2 Backups are managed in line with the organization ICT policy and industry best practice 7.3 Database backups are updated as per the ICT policy 7.4 Backups are stored as per the organization set up and industry best practice 7.5 Backups are regularly checked in line with the ICT policy 7.6 Identify and manage backup solutions in line with the organization policy

RANGE

This section provides work environments and conditions to which the performance criteria apply. It allows for different work environments and situations that will affect performance.

Variable	Range
	•

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Troubleshooting techniques
- ICT Infrastructure auditing procedures
- ICT safety and precautious measures
- ICT Prevention measures

• Performance monitoring techniques • ICT policy • Causes of hardware and software failure • Components of ICT Infrastructure • User training procedures

FOUNDATION SKILLS

The individual needs to demonstrate the following additional skills:	
• Communications (verbal and written); • Proficient in ICT; • Time management; • Analytical • Faults troubleshooting • Problem solving; • Planning;	• Decision making; • Report writing;

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required skills and understanding and range.

1. Critical Aspects of Competency	Assessment requires evidence that the candidate: 1.1 Database was established as per amount of data it holds 1.2 Database was identified as per its operation model 1.3 Cost evaluation was performed in database type identification 1.4 Database was checked for misconfiguration in line with the manufacturers guide 1.5 Database patches were deployed in a test environment as per the organization quality assurance policy. 1.6 Database patches were monitored as per the ICT policy 1.7 Hardware sizing was performed in line with database to be secured 1.8 Database firewall was configured as per the database expected operation 1.9 Automatic backups were scheduled as per the ICT policy and regulations 1.10 Backups were managed in line with the organization ICT policy and industry best practice 1.11 Backups were stored as per the organization set up and industry best practice

2. Resource Implications for competent certification	The following resources should be provided: 2.1 Access to relevant workplace where assessment can take place 2.2 Appropriately simulated environment where assessment can take place 2.3 Materials relevant to the proposed activity or tasks
3. Methods of Assessment	Competency may be assessed through: 3.1 Oral questioning 3.2 Practical demonstration 3.3 Observation
4. Context of Assessment	Competency may be assessed individually in the actual workplace or through simulated work environment
5. Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.