Introduction.

This is a report that refers to the Helpdesk database and assess its technical suitability in terms of data security, availability and integrity. It makes recommendation where required.

Database Security.

“Data is a valuable resource that must be strictly controlled and managed, as must any corporate resource. Part or all of the corporate data may have strategic importance to an organization and should, therefore, be kept secure and confidential.” [1]

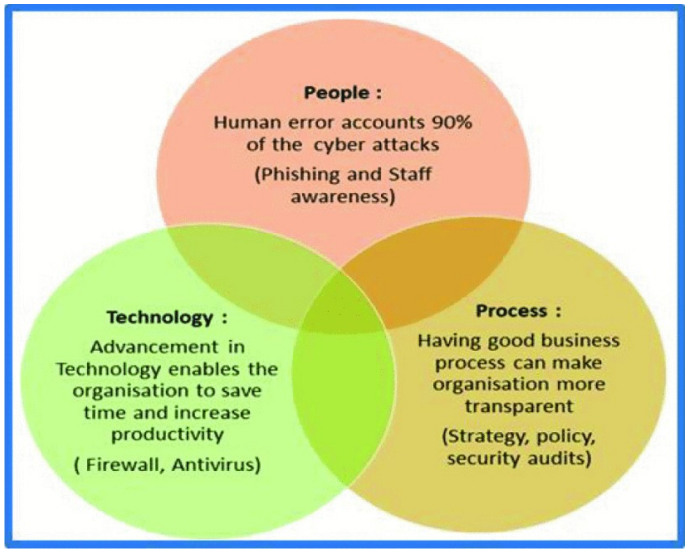

Fig 1.0

A SWOT analysis [6] was carried out by the Helpdesk development team. Some common Threats [7] (SWO**T)** were broken out with Overall Consequences levels assigned.

			Overall Consequences			
		Impact	**Minor** Database available but with some deviations	**Moderate** Database unavailable >20mins. Possible Data integrity issue.	**Major** Database unavailable >2 Hours. Data integrity issue.	**Severe.** Database unavailable >1 day. Data integrity/corruption.
Likelihood	**Almost Certain**	Expected to occur >1 time in the future.	Medium	Large	Very Large	Very Large
	Likely	Expected to occur at some stage.	Medium	Large	Large	Very Large
	Possible	May occur in future.	Medium	Medium	Medium	Large
	Unlikely	Not likely in normal circumstances	Low	Medium	Medium	Medium
	Rare	Could happen but not probable	Low	Low	Low	Medium

Table1A

Threat Number.			**Likely Hood**	**Impact**	**Overall Consequences**
	Hardware				
1		Part Fail	Likely	Major	Large
2		Power surge	Likely	Major	Large
3		Act God (weather, flooding etc)	Possible	Severe	Large
4		Theft	Possible	Major	Medium
	Software				
5		Malware	Possible	Moderate	Medium
6		End support/Forced upgrade	Likely	Minor	Medium
7		SQL injection	Possible	Major	Medium
	Users				
8		Shared Logins	Likely	Moderate	Large
9		Virus	Likely	Severe	Very Large
10		Human Error	Almost certain	Major	Very Large
11		Excessive privledges	Likely	Severe	Very Large

Table1B.

Oracle provides two types of security, [1] [2];

System security – access to the database for authorized users only [1].

The Helpdesk features both Apple and Microsoft OS. Both feature 2FA [4,5] through phone/email and this was considered as a method to authenticate from the OS to Oracle.

The risk here is that updates to the OS or newly added equipment that does not support this feature would render the database unaccessible.

The Helpdesk is an internal system (not public facing) that has just employee access. Oracles own stand-alone database authentication can be used and includes;

Password Encryption, Account Locking, Password Lifetime, Expiration +Complexity Verification [2].

Point 8, table 1B is still relevant but this can be mitigated against in company security policies.

Data security – through Discretionary access control (DAC) [citation].

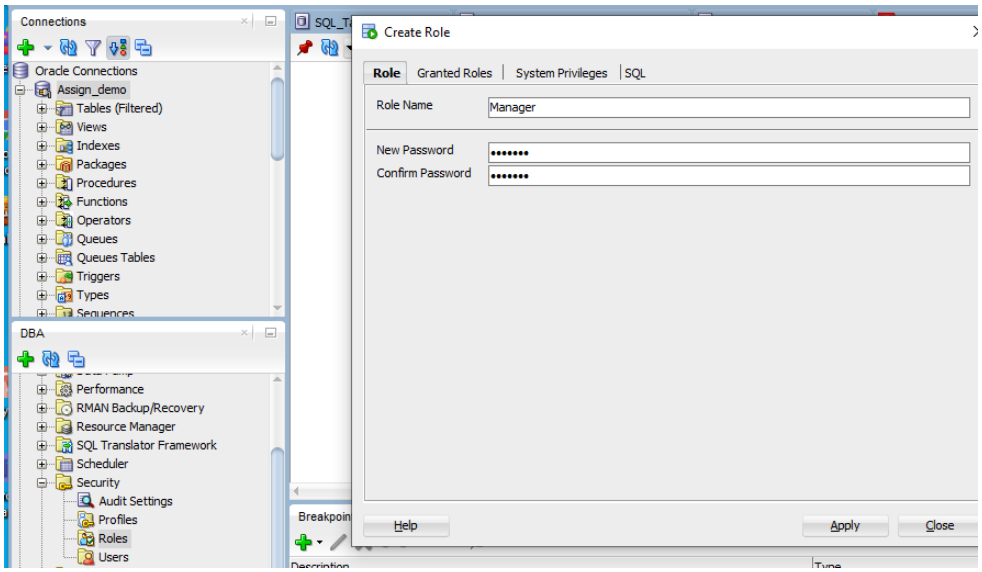

Fig 1. Creating a Manager role using SQL developer.

[1] T.M, Connolly; C.E, Begg, Database Systems - A Practical Approach to Design Implementation and Management, PP623, Pearson Education, 2015.

[2] A. H. Khan, P. Bahl Sawhney, S. Das, and D. Pandey, 'SartCyber Security Awareness Measurement Model (APAT)', in 2020 International Conference on Power Electronics IoT Applications in Renewable Energy and its Control (PARC), Feb. 2020, pp. 298–302, doi: 10.1109/PARC49193.2020.236614

[3]'Database Concepts'. https://docs.oracle.com/cd/B19306_01/server.102/b14220/security.htm (accessed Nov. 01, 2020).

[4] W. D. Blog, 'Convenient two-factor authentication with Microsoft Passport and Windows Hello', *Windows Developer Blog*, Jan. 26, 2016. https://blogs.windows.com/windowsdeveloper/2016/01/26/convenient-two-factor-authentication-with-microsoft-passport-and-windows-hello/ (accessed Nov. 06, 2020).

[5] 'Two-factor authentication for Apple ID', *Apple Support*. https://support.apple.com/en-gb/HT204915 (accessed Nov. 01, 2020).

[6] 'ProjectManagement.com - SWOT Analysis'. https://www.projectmanagement.com/wikis/233091/SWOT-Analysis (accessed Nov. 07, 2020).

[7] ‘Database Security: An Essential Guide’, Dec. 13, 2019. https://www.ibm.com/cloud/learn/database-security (accessed Nov. 06, 2020).