CORE HR and ERP GO LIVE RISKS

INDEX	AREA	SCENARIO	CURRENT RISK	RESIDUAL RISK (Y,N) AND DESCRIPTION OF RISK	LIKLIHOOD (H/M/L)	IMPACT (H/M/L)	POLICY AND PROCESS
1	Technical access	User access system via remote desktop	User emails finance and HR reports/information outside the network to an unmanaged device (against policy).	N. Users would continue to do this	n/a	n/a	Existing policy suffices but project should remind staff of their obligations
2	Technical access	Lewisham staff access system on unmanaged device via a web browser	n/a	Y. User can download data locally directly from the system and then if they lose device the Council has no way to wipe this remotely. Likliehood of them downloading	M	M	Policy that they should (a) not download data locally and (b) only access systems on devices managed by IMT.
3	Technical access	Lewisham staff access system on unmanaged device via a web browser	n/a	Y. Mobile devices have less protection against malware i.e. screenscraping login details.	L	?	Policy that staff should only access systems on devices managed by IMT
4	Technical access	User accesses system from managed device	User can download data locally (e.g. HR or finance data) and then lose the device. Unlike the above, these devices can be wiped	N. Users already have access to this data on mobiles via email	n/a	n/a	n/a
5	User access	Non permitted staff member given access to the system	Staff leave but continue to have access to the system to view data	N. Reduced risk as access is linked to role. If a person replaces a member of staff their permissions are transferred.	n/a	n/a	n/a
6	Data security	Lewisham staff given the wrong role	Lewisham user receives wrong role in the system and can see sensitive data (and carry out transactions) unrelated to their role	N. As now roles and data access are authorised by the data owner. There is no auto provisioning of roles for any employees so the risk remains the same	n/a	n/a	n/a
7	Data security	'Collateral intrusion'' - data can be viewed by user who should not be able to access it		Y as an integrated system. HR data can be viewed by finance			
8	Data security	Third parties accessing the system e.g. schools	The same data loss risks as for Lewisham employees, however the third party owns the risk not us	N.	n/a	n/a	n/a
9	Data security	Data at rest in Oracle Fusion	Data at rest is compromised - either digitally or physically	N. System complies with the government’s ‘Cloud Security Principles’ and best practices. Encryption is optional and is not an essential requirement.	n/a	n/a	Oracle owned

10	Data security	Data in transit	If the data is not protected, it could be intercepted or stolen	N. Data will be encrypted. Assurance on encryption provided by Blackberry in March 2018	n/a	n/a	RICHARD

SOLUTIONS	
PEOPLE (TRAINING AND GUIDANCE)	TECHNOLOGY
Project should remind staff as part of the comms, as we did with phase two rollout	n/a
Staff education and training. Online DP training with explicit reference to mobile working	Two options: (a) a brokerage technology which provides additioanl controls to user accounts. (b) whitelisting continues in place until
n/a	Oracle owned
n/a	n/a
n/a	n/a
n/a	n/a
n/a	n/a
Oracle owned	Oracle have implemented a range of controls, assured by the Oracle secuirty working group

RICHARD	Data will be encrypted in transit end to end using secure data transfer protocol (HTTPS / SFTP key length 128 bit).