Application / Solution:		**ESSI Money Game**	
Vendor name:	Financial Basics Foundation		
Description:	ESSI Money Game v2.0		
Report date:	May 2021	**Questionnaire submission date:**	09/04/2021
Intended users:	Teachers	**Licensing model:**	Other
Data sensitivity rating:	**No framework**	**Consent to share results: ***	Yes
Initial risk rating:	**Yellow**		
Overall risk rating:	**Yellow**		

**Vendors were asked if they were willing to share the assessment data and results with other educational jurisdictions in Australia*

Information Types Stored/Managed by Solution

Staff/teacher name	*X*	*Student email address*	*X*	*Student biometric data*	
Staff/teacher email address	*X*	*Student date of birth*		*Student geolocation data*	
Staff/teacher personal information		*Student work/content*		*Student grades or performance data*	
School Name	*X*	*Student attendance records*		*Student other data*	
Staff/teacher other data	*X*	*Student behavioural records*		*Parent name*	
Student name	*X*	*Student photos or videos*		*Parent contact information*	
Student home address		*Student gender*	*X*	*Parent financial data*	
Student telephone number		*Student medical or health data*		*Parent other data*	

Risk Area & Recommendations

Area	Rating	Description
Governance	**Amber**	The Supplier maintains some aspects of security governance over the operations of the service provided to DOE, but there are noted gaps against security best practice specifically around published policies, standards and embedded practices and processes. Questions that contributed to this rating include: • *COM10 – Maintain an ISMS –* ***No*** • *COM11 – CISO or CSO –* ***Role does not exist*** • *COM13 – Security related policies and standards* • *DSE2 – Data classification schema* • *DSE7 – Police background checks (employees/contractors) –* ***Other*** • *SEC3 – Security assessment results available to customers –* ***Not provided***
Supply Chain Risk Management	**Yellow**	Supply chain risk is mostly well-managed with some minor exceptions noted relating to how 3rd parties handle or store information or provide support services to the Supplier. Questions that contributed to this rating include: • *SOL1 – Hosting solution architecture –* ***via a public cloud provider (such as AWS)*** • *SOL7 – Usage of third-party software code –* ***Solutions utilises open source code/solution/service*** • *SOL8 – Management of third-party software code –* ***Other***

Access & Authorisation	**Amber**	Access to systems, locations and data used by the Supplierâ€™s solution is managed but with some weaknesses identified. To ensure the continued confidentiality and integrity of user information, further process and configuration enhancements are required, especially around identification, authentication, authorisation and credential/password management. Questions that contributed to this rating include: • *SOL3 – Physical access to infrastructure and data –* ***Administrative staff of external/3rd party/hosting provider*** • *DSE4 – Control of access to stored data –* ***Role based access control*** • *DSE6 – Securing admin accounts –* ***Technical controls*** • *DSE8 – Prevention of unauthorised access to data –* ***Not ascertainable*** • *DSE9 – Prevention of copying or theft of data –* ***No controls in place*** • *ACC4 – Account management –* ***Vendor*** • *ACC5 – Storage of user credentials –* ***Password hashing (without encryption)*** • *ACC7 – Multi-factor authentication (MFA) deployed –* ***No support for MFA***
Data Security	**Green**	The supplier demonstrates a sufficient level of compliance within this category area.
Security Monitoring & Incident Mgmt	**Amber**	Some of the process, practices and systems used to detect and respond to adverse security events and incidents are in place but are below the levels required for effective risk management. Policy and procedural enhancement, as well as the deployment of robust detection systems are required to achieve a satisfactory maturity for incident management. Questions that contributed to this rating include: • *LOG1 – System logging –* ***Yes - Minimal logging*** • *LOG2 – Length of system log retention –* ***Logs retained for maximum 30 days*** • *LOG4 – Security logging –* ***Yes - Minimal logging (some elements of the solution)*** • *LOG5 – Length of security log retention –* ***Logs retained for maximum 30 days*** • *SEC1 – Vulnerability assessments performed –* ***Other*** • *SEC2 – Penetration testing performed –* ***Other***
Privacy	**Yellow**	Some minor issues were noted relating to how privacy related data is managed. Compliance requirements for managing this information is defined in the Australia Privacy Principles (APP) and the Privacy Act (1988). Failure to fully comply with the act can have consequences such as the increased likelihood of suffering a privacy breach and incurring regulatory fines and reputational loss of business. Questions that contributed to this rating include: • *COM12 – Data Privacy Officer (DPO) –* ***Role does not exist*** • *DSE10 – Sharing of data with external groups –* ***Yes*** • *ACC11 – Online publicly browsable profile for users –* ***Yes - In solution only*** • *DAT2 – Process for user to request a complete copy of their data*
Solution Maturity	**Yellow**	Some minor issues were identified with the maturity of the service or solution provided by the Supplier in respect to the management of the data and the integration of security with solution design. The end to end use of data by the solution, its retention and storage, and the use of contingency plans for security incidents requires enhancement for full compliance. Questions that contributed to this rating include:

		• *COM14 – Business Continuity/Incident Mgt/ Data Breach Plans* • *COM17 – Policies written in child-friendly format – **No*** • *DAT4 – Data retention (including backups) – **Greater than one year***
Legal & Contractual	**Green**	The supplier demonstrates a sufficient level of compliance within this category area.