Control	Assessment Questions	Yes	No	N/A	Notes
RISK MANAGEMENT	*Would there be impact if the system were compromised, particularly regarding monetary damage, reputational damage, and contractual or regulatory obligations?*		✔		Ulyngo stores no confidential information. If our system was compromised, your university would not incur monetary or reputational damages.
	What other systems or process are dependent on this system?			✔	No systems are dependent on Ulyngo's systems
GENERAL INFORMATION	*Has your application security controls been tested by a third party?*	✔			Stripe is our payment processor and has been audited by an independent PCI Qualified Security Assessor (QSA) and is certified as a PCI Level 1 Service Provider.
	Please provide a copy of your SSAE 16 for review.				Heroku and the AWS infrastructure powering Heroku are: SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II) compliant. Details on Heroku and AWS security can be found here and here. Please note that Heroku and AWS security documents may require an NDA between the University and both Heroku and AWS. Security whitepaper's on both AWS and Heroku can be provided upon request.
AUTHORIZATION	*Please describe your authorization process for a user to get access to your system or application.*	✔			A user signs in with their student ID via SSO and then is redirected to Ulyngo's privately hosted platform.

	How do you ensure segregation of duties that limits functional access by assigned role that allows only authorized personnel to have access to have access to specific date?				We have clear roles between the team and we utilize Google Apps and Amazon IAM to manage acres and security.
AUTHENTICATION	*How is user authentication performed?*				Ulyngo's SAML SP integrates with your Universities SSO IdP to verify and authenticate each user.
	Does the system enforce a password policy for password complexity, required password expiration and initial password handling?		✔		No. Users sign in with their student ID via your university and any password management would come from the universities system.
	Is password transmission and storage encrypted and not viewable even to the system administrators?	✔			We do not store any password information.
	Does the application automatically log a user off the application after a predefined period of inactivity?	✔			Our TTL is directly tied to the TTL that your university assigns with their SSO sessions.
CLASSIFYING DATA	*Is any of the data maintained by this system subject to federal regulations such as HIPAA, FERPA, or GLBA?*		✔	✔	Not applicable.

	Is any of the data maintained by this system subject to PCI-DSS?	✔			Stripe stores all payment data and is our payment provider. Stripe has been audited by an independent PCI Qualified Security Assessor (QSA) and is certified as a PCI Level 1 Service Provider.
	What data does Ulyngo collect?				Ulyngo only stores: - First Name - Last Name - Address - Email Address - Birth date - Uploaded media by a user - Site activity history (products purchased, items listed, etc.)
AUDITING CAPABILITIES	*Is audit log tracking a feature available in the current version of this software application?*	✔			Via AWS CloudTrail and GitHub Audit Tools.
	Does the logging capture user access activity such as successful logon, logoff, and unsuccessful logon attempts?			✔	We track when a user logs out of Ulyngo but all log in functions are handled by the university.
	Does the logging capture data access inquiry activity such as screens viewed and reports printed?	✔			Via Mixpanel.
	Does the logging capture data entries, changes, and deletions?	✔			Via Mixpanel.
	Indicate how audit log files are protected from			✔	Limiting read access to the access logs only by authorized personnel.

	unauthorized alteration.				AWS CloudTrail is also PCI 10.5.2 which protects audit trail files from unauthorized modifications.
	How long logs are kept?				By default, log files are stored indefinitely.
CHANGE CONTROL	*Can you please describe the change control procedures for the software/ application under review?*				1. We define the change request (what the specific change is, reason for the change, conditions of success, expected completion timeline, value tec.) 2. Submit and review the change request to VP or Product and VP of Engineering 3. Create Proposal Document to universities and partners that would be affected by change (Proposed solution, proposed timeline, Impacts to the project, expiration date for proposed changes, etc.) 4. Final decision and approval
	Are written policies and procedures in place for making changes to your source control?	✔			Yes. Any changes to our source control are brought to our VP of Engineering. They are then pushed to staging for review and approval. Once approved, the changes will implemented. Source control managed via Github.
DATA PROTECTION	*Please describe how school data is encrypted at rest for files and databases.*				AWS hosts our server and provides the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data. More info here. SSL certified to provide secure, encrypted communications between our platform and any internet browser.
	How are data transmissions secured from our school to vendor?			✔	No data files are requested

	Once data files are received and processed, how long are they retained?			✔	No data files are requested
BACKUP AND RECOVERY	*What method is used to backup data and applications?*				AWS performs our data backup and recovery. Their methods include: • File-level recovery • Volume-level recovery • Application-level recovery (for example, databases) • Image-level recovery To learn more about our Backup and Recovery Approaches using AWS, click here.
	How often are backups performed? How long are they retained?				Amazon RDS performs a full daily backup of our. Our backups are retained for 35 days after the automated backup.
	Are backups stored offsite?				Yes
PHYSICAL SECURITY	*Is access to central systems physically controlled and restricted?*	✔			Our data centers, by AWS, are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. For more info, click here.
DOCUMENTATIO N	*Does the application include documentation that explains error or messages to users and system administrators and information on what actions required?*	✔			
FERPA	*Please Describe the FERPA controls that are in place for your application.*			✔	

BREACH INSURANCE	*Does your company carry breach insurance?*	✔			Yes
	Do you have a certificate you can share.	✔			Yes, upon request.